

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2005 年 8 月 4 日 (04.08.2005)

PCT

(10) 国際公開番号
WO 2005/071880 A1

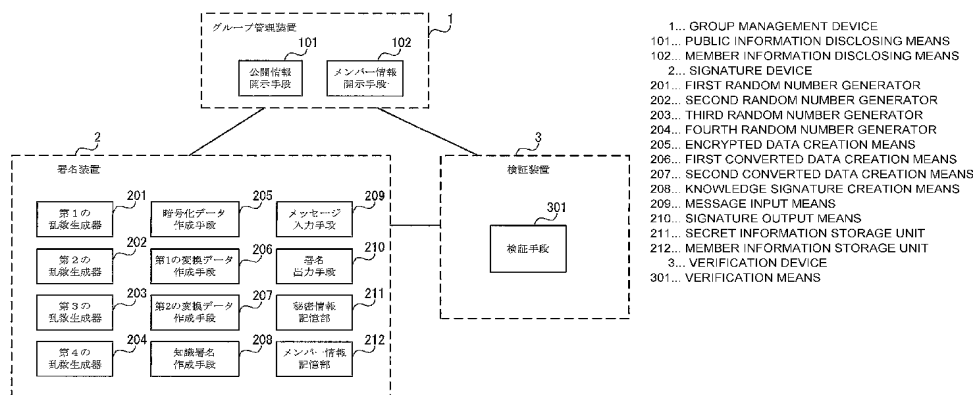
- (51) 国際特許分類⁷: H04L 9/32, G09C 1/00
- (21) 国際出願番号: PCT/JP2005/001177
- (22) 国際出願日: 2005 年 1 月 21 日 (21.01.2005)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2004-016006 2004 年 1 月 23 日 (23.01.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目 7 番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 米澤 祥子 (YONEZAWA, Shoko) [JP/JP]; 〒1088001 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内 Tokyo (JP). 古

- 川 潤 (FURUKAWA, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内 Tokyo (JP).
- (74) 代理人: 松本 正夫 (MATSUMOTO, Masao); 〒1710021 東京都豊島区西池袋二丁目 3 6 番 1 0 号 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE,

[続葉有]

(54) Title: GROUP SIGNATURE SYSTEM, METHOD, DEVICE, AND PROGRAM

(54) 発明の名称: グループ署名システム、方法、装置、およびプログラム



(57) **Abstract:** A signature device (2) encrypts a first element of a member certificate by using a first random number and public information disclosed by a group management device (1) so as to generate encrypted data. Moreover, the signature device (2) converts the first element by using a random number and the public information so as to create first and second converted data. Moreover, the signature device (2) creates knowledge signature data from which the first element, the second element, and the information on the signature key will not be known and outputs a group signature including it together with a message. A verification device (3) verifies whether the group signature has been created by using a member certificate and a signature key of a member registered in the group.

(57) 要約: 署名装置 (2) は、メンバー証明書第 1 の要素を第 1 の乱数とグループ管理装置 (1) にて開示されている公開情報とを用いて暗号化して暗号化データを作成する。また、署名装置 (2) は、第 1 の要素を乱数および公開情報を用いて変換して第 1、第 2 の変換データを作成する。そして、署名装置 (2) は、第 1 の要素、第 2 の要素、および署名鍵に関する情報を知られることのない知識署名データを作成し、それを含むグループ署名をメッセージと共に出力する。検証装置 (3) は、メッセージおよびグループ署名と公開情報とから、グループ署名が、グループに登録されているいずれかのメンバーのメンバー証明書および署名鍵を用いて作成されたものか否かを検証する。



BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,
IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR),
OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される
各*PCT*ガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

明細書

グループ署名システム、方法、装置、およびプログラム

5 技術分野

本発明は、グループに所属するメンバーが、グループのメンバーであることを証明するための署名を作成し、また検証するグループ署名システムに関し、特に、グループ管理者の処理権限を複数に分散する機能を有するグループ署名システムに関する。

10

背景技術

従来、この種のグループ署名システムは、複数のメンバーから構成されるグループにおいて、グループに所属する、あるユーザが署名を作成し、またその署名を検証するためのものである。そして、その署名は、署名者がグループのいずれかのメンバーであることは検証できるが、通常ではグループ内のどのメンバーであるかは分からないという性質のものである。ただし、その一方で、万が一のために、署名から実際の署名者を特定する機能（以下、追跡と称す）がグループ署名システムには備えられている。

一般に、グループ署名システムでは、グループ管理者と呼ばれるエンティティがグループ内に存在し、グループへの新たなメンバーの登録手続きおよび署名者の追跡を行う。その場合、グループ署名システムにおいて、グループへのメンバーの登録や、グループ署名の署名者追跡は、全てグループ管理者の権限で行われることとなる。このように、これら全ての権限を単一のグループ管理者に与えてしまうことがシステムの安全上好ましくない場合がある。

グループ管理者が不正を働こうとすれば、このグループ署名システムは不正を防止することができない。例えば、グループ管理者がメンバーを不正に追加し、そのメンバーを利用して、署名者の特定できない署名を作成することができてしまう。

このような不正が行なわれる可能性をできる限り低減し、グループ署名システ

ムの信頼性を向上させるために、単一のグループ管理者に全ての権限を与えることをせず、複数のエンティティでグループ管理者の役割を担うことが考えられる。

従来のグループ署名システムにおいては、グループ管理者の機能を、新たなユーザをグループに登録する権限を持つメンバー管理者と、グループ署名の署名者を特定する権限を持つメンバー追跡者に分割することが提案されている。G. Ateniese and R. de Medeiros, "Efficient Group Signatures without Trapdoors," In Advances in Cryptology--ASIACRYPT 2003, LNCS 2894, pp. 246-268, Springer-Verlag, 2003. (以下、文献1) および、G. Ateniese, J. Camenisch, M. Joye and G. Tsudik, "A Practical and Provable Secure Coalition-Resistant Group Signature Scheme," In Advances in Cryptology--CRYPTO2000, LNCS 1880, pp. 255-270, Springer-Verlag, 2000. (以下、文献2) で示されるグループ署名システムでは、このようなグループ管理者の分割が考慮されている。

また、そのメンバー管理者とメンバー追跡者の信頼性を更に向上させるために、メンバー管理者およびメンバー追跡者の各々の権限をさらに複数エンティティに分散し、複数のメンバー管理者あるいはメンバー追跡者が協力してそれら機能を果たすことも考えられている。

文献1にて提案された第1の従来技術において、メンバー管理者の用いる公開鍵と秘密鍵は、ElGamalによる"A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms" (IEEE Trans. on Information Theory, IT-31, 4, pp. 469-472) に記載されているように、有限体上の乗法群の離散対数問題に基づく暗号系から選択される。また、文献2で提案された第2の従来技術においては、メンバー管理者の用いる公開鍵と秘密鍵は、RSA暗号("A Method f

or Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, Vol. 21, No. 2, pp. 120–126) のような暗号系に基づいて選択される。

5 文献 1 に記載された第 1 の従来技術のグループ署名システムは、公開情報開示手段と署名装置とを有している。図 13 は、第 1 の従来技術のグループ署名システムにおける署名装置の構成を示すブロック図である。図 13 を参照すると、署名装置は、第 1 の乱数生成器 1201、第 2 の乱数生成器 1202、第 3 の乱数生成器 1203、第 4 の乱数生成器 1204、第 5 の乱数生成器 1205、第 6
10 の乱数生成器 1206、第 1 の暗号化データ作成手段 1207、第 2 の暗号化データ作成手段 1208、第 1 の変換データ作成手段 1209、第 2 の変換データ作成手段 1210、知識署名作成手段 1211、秘密情報記憶部 1212、メンバー情報記憶部 1213、メッセージ入力手段 1214 および署名出力手段 1215 から構成されている。

15 第 1 の乱数生成器 1201 は、第 1 の暗号化データ作成手段 1207 で使用する乱数を生成する。

第 2 の乱数生成器 1202 は、第 2 の暗号化データ作成手段 1208 で使用する乱数を生成する。

20 第 3 の乱数生成器 1203 は、第 1 の変換データ作成手段 1209 で使用する乱数を生成するとともに、その乱数をグループ署名の要素として署名出力手段 1215 に出力する。

第 4 の乱数生成器 1204 は、第 2 の変換データ作成手段 1210 で使用する乱数を生成するとともに、その乱数をグループ署名の要素として署名出力手段 1215 に出力する。

25 第 5 の乱数生成器 1205 は、第 2 の変換データ作成手段 1210 で使用する乱数を生成するとともに、その乱数をグループ署名の要素として署名出力手段 1215 に出力する。

第 6 の乱数生成器 1206 は、知識署名作成手段 1211 で使用する乱数を生成する。

第1の暗号化データ作成手段1207は、第1の乱数生成器1201で生成された乱数と、メンバー情報記憶部1212に記憶されているメンバー証明書の第1の要素とを入力として、メンバー証明書の第1の要素の暗号化データ（以下、第1の暗号化データと称す）を知識署名作成手段1211および署名出力手段1215に出力する。

第2の暗号化データ作成手段1208は、第2の乱数生成器1202で生成された乱数と、秘密情報記憶部1213に記憶されている署名鍵の変換データとを入力として、署名鍵の変換データの第1の要素の暗号化データ（以下、第2の暗号化データと称す）を知識署名作成手段911および署名出力手段1215に出力する。

第1の変換データ作成手段1209は、第3の乱数生成器1203で生成された乱数と、メンバー情報記憶部1212に記憶されているメンバー証明書の第1の要素を入力として、メンバー証明書の第1の要素の変換データ（以下、第1の変換データと称す）を知識署名作成手段1211および署名出力手段1215に出力する。

第2の変換データ作成手段1210は、第4の乱数生成器1204および第5の乱数生成器1205で生成された乱数と、メンバー情報記憶部1212に記憶されているメンバー証明書の第1の要素を入力として、メンバー証明書の第1の要素の変換データ（以下、第2の変換データと称す）を知識署名作成手段1211および署名出力手段1215に出力する。

知識署名作成手段1211は、メッセージ入力手段1214から入力されたメッセージ、第6の乱数生成器1206で生成された乱数、第1の暗号化データ、第2の暗号化データ、第1の変換データ、第2の変換データ、メンバー証明書の第1および第2の要素、および署名鍵を入力として、メンバー証明書および署名鍵に関する情報を漏らすことなくメンバー証明書および署名鍵を正しく所有していることを証明することのできる知識署名データを出力する。

メンバー情報記憶部1212は、グループ署名を発行するために用いるメンバー証明書を記憶する。メンバー証明書は第1の要素と第2の要素とからなる。

秘密情報記憶部1213は署名鍵を記憶する。

メッセージ入力手段 1 2 1 4 は、署名を付加すべきメッセージを入力する。

署名出力手段 1 2 1 5 は、メッセージ、第 1 の暗号化データ、第 2 の暗号化データ、第 1 の変換データ、第 2 の変換データ、第 3 の乱数、第 4 の乱数、第 5 の乱数、および知識署名データをグループ署名として出力する。

5 以上の構成により、第 1 の従来技術のグループ署名システムはグループ署名を作成することができる。

一方、文献 2 に記載された第 2 の従来技術のグループ署名システムは、グループ管理装置および署名装置を有している。

10 グループ管理装置は公開情報開示手段、メンバー情報開示手段、R S A 鍵生成手段、離散対数鍵生成手段、メンバー登録秘密情報記憶部、メンバー追跡秘密情報記憶部、およびメンバー登録手段を有している。そして、グループ管理装置は、グループメンバーの登録処理や、与えられた署名から実際の署名者の特定処理を行う。

公開情報開示手段は、システムで用いる公開情報をすべての装置に開示する。

15 メンバー情報開示手段は、メンバー登録手段で取得した署名装置に関する情報を開示する。

R S A 鍵生成手段は、R S A 暗号系による方法で公開鍵および秘密鍵を作成し、公開鍵を公開情報開示手段に出力し、秘密鍵をメンバー登録秘密情報記憶部に出力する。

20 離散対数鍵生成手段は、離散対数問題に基づく暗号系から公開鍵および秘密鍵を作成し、公開鍵を公開情報開示手段に出力し、秘密鍵をメンバー追跡秘密情報記憶部に出力する。

メンバー登録秘密情報記憶部は、R S A 鍵生成手段で作成した秘密鍵を記憶する。

25 メンバー追跡秘密情報記憶部は、離散対数鍵生成手段で作成した秘密鍵を記憶する。

メンバー登録手段は、メンバー登録秘密情報記憶部に記憶された秘密鍵を入力として、グループ署名を作成するのに必要なメンバー証明書を署名装置に対して出力する。

一方、署名装置は、グループ管理装置から取得したメンバー証明書を用いてグループ署名を作成する。

そして、第2の従来技術によるグループ管理装置はメンバー管理装置とメンバー追跡装置に分割されてもよい。その場合、メンバー管理装置はRSA鍵生成手段、メンバー登録秘密情報記憶部、およびメンバー登録手段を有し、メンバー追跡装置は離散対数鍵生成手段、メンバー追跡秘密情報記憶部を有することとなる。

第1の問題点は、第1の従来技術において、グループ管理装置をメンバー管理装置とメンバー追跡装置に機能分割すると、メンバー管理装置が実際の署名者を特定する機能を有することになってしまう点である。

第1の従来技術では、第1の変換データ作成手段1209で作成される第1の変換データは、第3の乱数生成器1203で生成される乱数（以下、第3の乱数と称す）とメンバー証明書の第1の要素とに依存する確定的な値であり、かつ第3の乱数は後にグループ署名の要素として公開される。そのため、メンバー管理装置は、開示されたすべてのメンバー証明書の情報と、グループ署名の要素として開示された第3の乱数とを入力として、全てのメンバー証明書について総当りで第1の変換データ作成手段1209と同じ変換を行い、署名装置から出力されたグループ署名に含まれた第1の変換データと一致する値が得られたときのメンバー証明書の持ち主を調べれば、署名者を特定できてしまう。

第2の問題点は、第2の従来技術において、メンバー管理装置の処理権限を複数エンティティに分散する場合、複数のエンティティに大きな負荷がかかり、効率的でないという点である。

第2の従来技術では、メンバー管理装置の用いる秘密鍵はRSA暗号系に基づいて選択されているが、一般にRSA暗号系の分散計算は複雑で、計算量が大きいことが知られている。そのため、この大きな計算量による負荷が複数のエンティティにかかることとなる。

本発明の目的は、グループ署名からメンバー証明書に関する情報を秘匿できるグループ署名を提供し、また、グループ管理装置の機能を安全確実にメンバー管理装置とメンバー追跡装置に分割することができ、さらに、メンバー管理装置およびメンバー追跡装置の機能を効率良く複数のエンティティに分散させることの

できるグループ署名システムを提供することである。

発明の開示

上記目的を達成するために、本発明のグループ署名システムは、署名者がグループに登録されたメンバーであることを証明することのできるグループ署名を作成し、また、作成された前記グループ署名の前記署名者が前記グループのメンバーであるか否か確認するグループ署名システムであって、

システム内で共通に利用する公開情報を他の装置から参照可能に開示するグループ管理装置と、

第1の要素および第2の要素を含むメンバー証明書を記憶しており、前記第1の要素を第1の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成し、前記第1の要素を第2の乱数および前記公開情報を用いて変換して第1の変換データを作成し、前記第1の要素を第3の乱数および前記公開情報を用いて変換して第2の変換データを作成し、署名を付加すべきメッセージ、第4の乱数、前記暗号化データ、前記第1の変換データ、前記第2の変換データ、署名の作成に用いる秘密鍵である署名鍵、前記第1の要素、および前記第2の要素から、知識署名データを作成し、前記暗号化データ、前記第1の変換データ、前記第2の変換データ、および前記知識署名データをグループ署名として前記メッセージと共に出力する署名装置と、

メッセージおよびグループ署名と、前記グループ管理装置にて開示されている前記公開情報とから、前記グループ署名が、前記グループに登録されているいずれかのメンバーのメンバー証明書に含まれる第1の要素および第2の要素と前記署名鍵を用いて作成されたものか否かを検証する検証装置とを有している。

また、前記署名装置は、前記暗号化データ、前記第1の変換データ、および前記第2の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第1の要素、前記第2の要素、および前記署名鍵に関する情報を知られることのないデータとして、前記知識署名データを作成し、

前記検証装置は、グループ署名が、前記グループに登録されているいずれかのメンバーのメンバー証明書に含まれる第1の要素および第2の要素と前記署名鍵

を用いて作成されたものか否かを、前記第1の要素、前記第2の要素、および前記署名鍵に関する情報を用いることなく、検証することとしてもよい。

また、新たなメンバーを前記グループに登録するとき、素数を位数とする有限体の元となるようにメンバー登録秘密鍵を選び、前記メンバー登録秘密鍵を離散対数とし、有限体上の乗法群の元であるメンバー登録公開鍵を前記メンバー登録秘密鍵から求め、前記メンバー登録公開鍵を公開情報として前記グループ管理装置に通知し、前記メンバー登録秘密鍵を自身で記憶すると共に、該メンバー登録秘密鍵を用いてメンバー証明書を作成し、前記署名装置に通知するメンバー管理装置をさらに有することとしてもよい。

また、前記メンバー証明書は、前記署名鍵を離散対数とする、前記署名鍵の変換データに対して前記メンバー登録秘密鍵を用いて作成したN y b e r g - R u e p p e l 署名であるとしてもよい。

また、前記グループ管理装置は、前記公開情報に加えて、前記メンバー管理装置から通知された前記メンバー情報を他の装置から参照可能に開示するものとしてもよい。

また、本発明のシステムは、新たなメンバーを前記グループに登録するとき、素数を位数とする有限体の所定の元の、複数に分散された値のうちの1つを自身の分散メンバー登録秘密鍵として割り当て、前記分散メンバー登録秘密鍵を自身で記憶すると共に、前記元を離散対数とする値をメンバー登録公開鍵とする、複数のメンバーサブ管理装置をさらに有し、

前記署名装置は、複数の前記メンバーサブ管理装置と通信することによりメンバー証明書を取得し、

前記グループ管理装置は、前記メンバー登録公開鍵を取得するものとしてもよい。

また、本発明のシステムは、素数を位数とする有限体の元となるようにメンバー追跡秘密鍵を選び、前記メンバー追跡秘密鍵を離散対数とし、有限体上の乗法群の元であるメンバー追跡公開鍵を前記メンバー追跡秘密鍵から求め、前記メンバー追跡公開鍵を前記公開情報として前記グループ管理装置に通知し、前記メンバー追跡秘密鍵を自身で記憶しておき、グループ署名の署名者を特定するとき、

前記グループ署名に含まれている暗号化データを前記メンバー追跡秘密鍵を用いて復号し、復号結果と前記グループ管理装置にて開示されているいずれかの前記メンバー証明書の第1の要素とが一致すれば該メンバー証明書のメンバーを署名者と特定するメンバー追跡装置をさらに有し、

5 前記グループ管理装置は前記メンバー証明書を前記メンバー情報として開示しており、

前記署名装置は前記第1の要素を暗号化して前記暗号化データを作成するとき前記公開情報として前記メンバー追跡公開鍵を用いることとしてもよい。

10 また、自身の分散メンバー追跡秘密鍵が、素数を位数とする有限体の元の複数に分散された値のうちの自身に割り当てる1つであり、メンバー追跡公開鍵が、前記有限体の元を離散対数とし、有限体上の乗法群の元となるように、前記分散メンバー追跡秘密鍵を求め、前記分散メンバー追跡秘密鍵を自身で記憶する複数のメンバーサブ追跡装置をさらに有し、

15 前記署名装置は前記第1の要素を暗号化して前記暗号化データを作成するとき前記公開情報として前記メンバー追跡公開鍵を用い、

前記グループ管理装置は前記メンバー証明書を前記メンバー情報として開示しており、

20 グループ署名の署名者を特定するとき、前記メンバーサブ追跡装置の各々が前記グループ署名に含まれている暗号化データに対して自身の前記分散メンバー追跡秘密鍵を用いて所定の計算をした結果から求まる復号結果と、前記グループ管理装置にて開示されているいずれかの前記メンバー証明書の第1の要素とが一致すれば該メンバー証明書のメンバーを署名者と特定することとしてもよい。

また、前記有限体上の乗法群に代えて楕円曲線上の有限群を用いることとしてもよい。

25 したがって、本発明によれば、署名装置が、メンバー証明書に関する情報を、グループ署名の要素として開示されない乱数を用いて秘匿することができる。また、メンバー管理装置の機能は複数のメンバーサブ管理装置に分散され、複数のメンバーサブ管理装置がメンバー証明書を計算するために使用する秘密鍵は、離散対数問題に基づく暗号系から選ばれる。また、メンバー追跡装置の機能は複数

のメンバーサブ追跡装置に分散され、複数のメンバーサブ追跡装置が署名者の特定に用いる秘密鍵は、離散対数問題に基づく暗号系から選ばれる。

図面の簡単な説明

5 図 1 は、第 1 の実施形態のグループ署名システムの構成例を示すブロック図である。

 図 2 は、第 1 の実施形態のグループ署名システムの他の構成例を示すブロック図である。

10 図 3 は、第 1 の実施形態のグループ署名システムのさらに他の構成を示すブロック図である。

 図 4 は、第 1 の実施形態の署名装置を構成する各ブロック間の関係を示す図である。

 図 5 は、第 1 の実施形態の署名装置およびメンバー管理装置を構成する各ブロック間の関係を示す図である。

15 図 6 は、第 1 の実施形態の検証装置内のブロックと他の装置との関係を示す図である。

 図 7 は、第 1 の実施形態のメンバー管理装置を構成する各ブロック間の関係を示す図である。

20 図 8 は、第 1 の実施形態のメンバー追跡装置を構成する各ブロック間の関係を示す図である。

 図 9 は、第 1 の実施形態のメンバー追跡装置を構成する各ブロック間の関係を示す図である。

 図 10 は、第 1 の実施形態によるグループ署名システムのメンバー登録時の動作を示すフローチャートである。

25 図 11 は、第 1 の実施形態による署名装置のグループ署名作成時の動作を示すフローチャートである。

 図 12 は、第 2 の実施形態のグループ署名システムの構成例を示すブロック図である。

 図 13 は、第 1 の従来技術のグループ署名システムにおける署名装置の構成を

示すブロック図である。

発明を実施するための最良の形態

本発明の一実施形態について図面を参照して詳細に説明する。

5 図 1 は、第 1 の実施形態のグループ署名システムの構成例を示すブロック図である。図 1 を参照すると、第 1 の実施形態のグループ署名システムは、グループ管理装置 1、署名装置 2、および検証装置 3 を有している。

10 なお、他の構成例として、第 1 の実施形態のグループ署名システムは、図 1 の構成に加えてメンバー管理装置を有してもよい。図 2 は、第 1 の実施形態のグループ署名システムの他の構成例を示すブロック図である。図 2 を参照すると、第 1 の実施形態のグループ署名システムは、図 1 の構成に加えて、メンバー管理装置 4 を有している。

15 さらに他の構成例として、第 1 の実施形態のグループ署名システムは、図 2 の構成に加えてメンバー追跡装置 5 を有してもよい。図 3 は、第 1 の実施形態のグループ署名システムのさらに他の構成を示すブロック図である。図 3 を参照すると、第 1 の実施形態のグループ署名システムは、図 2 の構成に加えて、メンバー追跡装置 5 を有している。

20 以下、メンバー登録機能とメンバー追跡機能の各々をグループ管理装置 1 から分割した図 3 のシステム構成例を用いて説明する。ただし、本発明はその構成に限定されるものではなく、それら機能を分割しない構成にも適用可能である。

図 3 を参照すると、グループ管理装置 1 は、公開情報開示手段 101、メンバー情報開示手段 102、および前処理手段 103 を有しており、システム全体で用いる公開情報を作成し、開示する。

25 署名装置 2 は、第 1 の乱数生成器 201、第 2 の乱数生成器 202、第 3 の乱数生成器 203、第 4 の乱数生成器 204、暗号化データ作成手段 205、第 1 の変換データ作成手段 206、第 2 の変換データ作成手段 207、知識署名作成手段 208、メッセージ入力手段 209、署名出力手段 210、秘密情報記憶部 211、メンバー情報記憶部 212、登録手段 213、および第 5 の乱数生成器 214 を有しており、メンバー登録の後、グループ署名を作成する。

検証装置 3 は検証手段 3 0 1 を有しており、与えられたグループ署名の正当性を確認する。

メンバー管理装置 4 は、離散対数鍵生成手段 4 0 1、メンバー登録秘密情報記憶部 4 0 2、メンバー登録手段 4 0 3、第 1 の乱数生成器 4 0 4、第 2 の乱数生成器 4 0 5 を有しており、グループメンバーの登録処理を行う。

メンバー追跡装置 5 は、離散対数鍵生成手段 5 0 1、メンバー追跡秘密情報記憶部 5 0 2、メンバー追跡手段 5 0 3、および乱数生成器 5 0 4 を有しており、与えられたグループ署名から実際の署名者を特定するメンバー追跡機能を有している。

グループ管理装置 1 において公開情報開示手段 1 0 1 は、前処理手段 1 0 3、離散対数鍵生成手段 4 0 1、離散対数鍵生成手段 5 0 1 から出力された各種の公開情報を記憶し、すべての装置が自由に参照できるように開示する。

メンバー情報開示手段 1 0 2 は、メンバー管理装置 4 のメンバー登録手段 4 0 3 と署名装置 2 の登録手段 2 1 3 とが互いに通信することにより作成されたメンバー情報を記憶し、すべての装置が自由に参照できるように開示する。

前処理手段 1 0 3 は、本システムで用いる共通の定数を予め定め、それを公開情報開示手段 1 0 1 に出力する。

図 4 は、第 1 の実施形態の署名装置を構成する各ブロック間の関係を示す図である。図 5 は、第 1 の実施形態の署名装置およびメンバー管理装置を構成する各ブロック間の関係を示す図である。

まず、図 4 において、第 1 の乱数生成器 2 0 1 は、暗号化データ作成手段 2 0 5 で使用する第 1 の乱数を生成する。

同様に、第 2 の乱数生成器 2 0 2 は、第 1 の変換データ作成手段 2 0 6 で使用する第 2 の乱数を生成する。第 3 の乱数生成器 2 0 3 は、第 2 の変換データ作成手段 2 0 7 で使用する第 3 の乱数を生成する。第 4 の乱数生成器 2 0 4 は、知識署名作成手段 2 0 8 で使用する第 4 の乱数を生成する。

暗号化データ作成手段 2 0 5 は、第 1 の乱数生成器 2 0 1 で生成した第 1 の乱数と、メンバー情報記憶部 2 1 2 に記憶されているメンバー証明書の第 1 の要素とを入力として、メンバー証明書の第 1 の要素を暗号化し、得られた暗号化デー

タを知識署名作成手段 208 および署名出力手段 210 に出力する。

第 1 の変換データ作成手段 206 は、第 2 の乱数生成器 202 で生成した第 2 の乱数と、メンバー情報記憶部 212 に記憶されているメンバー証明書の第 1 の要素とを入力として、メンバー証明書の第 1 の要素の変換データ（以下、第 1 の変換データと称す）を知識署名作成手段 208 および署名出力手段 210 に出力する。

第 2 の変換データ作成手段 207 は、第 3 の乱数生成器 203 で生成した第 3 の乱数と、メンバー情報記憶部 212 に記憶されているメンバー証明書の第 1 の要素とを入力として、メンバー証明書の第 1 の要素の変換データ（以下、第 2 の変換データと称す）を知識署名作成手段 208 および署名出力手段 210 に出力する。

知識署名作成手段 208 は、メッセージ入力手段 209 から入力されたメッセージ、第 4 の乱数生成器 204 で生成した第 4 の乱数、暗号化データ、第 1 の変換データ、第 2 の変換データ、秘密情報記憶部 211 に記憶されている署名鍵、メンバー情報記憶部 212 に記憶されているメンバー証明書の第 1 および第 2 の要素、公開情報開示手段 101 にて開示されている公開情報を入力として、メンバー証明書および署名鍵を所持していることを示す知識署名データを出力する。

メッセージ入力手段 209 は、署名を付加すべきメッセージを知識署名作成手段 208 および署名出力手段 210 に出力する。

署名出力手段 210 は、メッセージ入力手段 209 から入力されたメッセージ、暗号化データ、第 1 の変換データ、第 2 の変換データ、知識署名データをグループ署名として出力する。

秘密情報記憶部 211 は、署名に用いる秘密鍵である署名鍵を記憶する。

メンバー情報記憶部 212 は、メンバー管理装置 4 のメンバー登録手段 403 との通信を用いて取得したメンバー証明書を記憶する。

図 5 において、登録手段 213 は、メンバー管理装置 4 のメンバー登録手段 403 と通信を行い、また第 5 の乱数生成器 214 から出力された第 5 の乱数を入力として、メンバー管理装置 4 の署名を表すメンバー証明書と署名装置 2 の秘密情報である署名鍵とを取得し、前記メンバー証明書をメンバー情報記憶部 212

に、前記署名鍵を秘密情報記憶部 2 1 2 に、それぞれ出力する。第 5 の乱数生成器 2 1 4 は、登録手段 2 1 3 に入力する第 5 の乱数を生成する。

図 6 は、第 1 の実施形態の検証装置内のブロックと他の装置との関係を示す図である。

5 検証手段 3 0 1 は、与えられたグループ署名と、グループ管理装置 1 の公開情報開示手段 1 0 1 にて開示された公開情報とを入力として、グループ署名が署名装置 2 の署名出力手段 2 1 0 から正しく出力されたものか否か検証する。そして、検証手段 3 0 1 は、グループ署名が署名出力手段 2 1 0 から正しく出力されたものであるときのみ、そのグループ署名を受理し、そうでないときには、署名を不
10 受理とする。

これにより、検証手段 2 1 0 は、与えられたグループ署名が、ある署名装置が正しいメンバー証明書および署名鍵を使用して作成した正当なグループ署名であるか否かを検証し、正当なグループ署名であれば受理して署名受理の旨を出力し、そうでなければ不受理とし、署名不受理の旨を出力する。

15 図 7 は、第 1 の実施形態のメンバー管理装置を構成する各ブロック間の関係を示す図である。

図 7 を参照すると、離散対数鍵生成手段 4 0 1 は、第 1 の乱数生成器 4 0 4 から乱数を受け、その乱数を用いて、有限体上の乗法群の離散対数問題に基づく公開鍵と秘密鍵を計算し、秘密鍵をメンバー登録秘密鍵としてメンバー登録秘密情報記憶部 4 0 2 に記録し、公開鍵をメンバー登録公開鍵としてグループ管理装置
20 1 の公開情報開示手段 1 0 1 に出力する。

メンバー登録秘密情報記憶部 4 0 2 は、離散対数鍵生成手段 4 0 1 で作成した秘密鍵を記憶する。

第 1 の乱数生成器 4 0 4 は、離散対数鍵生成手段 4 0 1 に乱数を出力する。

25 図 5 を参照すると、メンバー登録手段 4 0 3 は、署名装置 2 の登録手段 2 1 3 と通信し、また第 2 の乱数生成器 4 0 5 からの乱数と、メンバー登録秘密情報記憶部 4 0 2 に記憶された秘密鍵とを入力として、署名装置 2 に対して第 1 の要素と第 2 の要素からなるメンバー証明書を発行し、また署名装置 2 との通信で得た署名装置 2 のメンバー情報をメンバー情報開示手段 1 0 2 に出力する。メンバー

証明書は、グループのメンバーであることを証明する情報であり、署名装置 2 がグループ署名を発行するときに用いられる。

第 2 の乱数生成器 4 0 5 は、メンバー登録手段 4 0 3 に乱数を出力する。

図 8 および図 9 は、第 1 の実施形態のメンバー追跡装置を構成する各ブロック間の関係を示す図である。

図 8 を参照すると、離散対数鍵生成手段 5 0 1 は、乱数生成器 5 0 4 から乱数を受け、その乱数を用いて、有限体上の乗法群の離散対数問題に基づく公開鍵と秘密鍵を計算し、秘密鍵をメンバー追跡秘密鍵としてメンバー追跡秘密情報記憶部 5 0 2 に記録し、公開鍵をメンバー追跡公開鍵としてグループ管理装置 1 の公開情報開示手段 1 0 1 に出力する。

メンバー追跡秘密情報記憶部 5 0 2 は、離散対数鍵生成手段 5 0 1 で作成した秘密鍵を記憶する。

乱数生成器 5 0 4 は、離散対数鍵生成手段 5 0 1 に乱数を出力する。

図 9 を参照すると、メンバー追跡手段 5 0 3 は、検証手段 3 0 1 で受理されたグループ署名と、メンバー情報開示手段 1 0 2 にて開示されているメンバー情報と、メンバー追跡秘密情報記憶部 5 0 2 に記憶されている秘密鍵を入力として、グループ署名の署名者を特定する。

以下、第 1 の実施形態のグループ署名システムの詳細動作について説明する。

まず最初に前処理として、前処理手段 1 0 3 が本システムで共通に用いる公開パラメータを設定する。ここで設定されたパラメータは、後に行われる、署名装置 2、メンバー管理手段 4、およびメンバー追跡手段 5 における鍵生成に用いられる。

前処理においては、まず第 1 の素数 p 、第 2 の素数 q 、第 3 の素数 P を選ぶ。

このとき、 p 、 q 、 P は、

$$q \mid p - 1, \quad p \mid P - 1$$

の関係を満たすように選ぶ。

p 、 q 、 P のビット数は、それぞれ

$$|q| \geq 160, \quad |p| \geq 1024, \quad |P| \geq 1024$$

が推奨される。

ここで、 p を位数とする乗法群 Z_p^* の、位数 q の部分群 G_q を考える。また、 P を位数とする乗法群 Z_P^* の、位数 p の部分群 G_p を考える。

そして、 G_p から第 1 の生成元 g 、第 2 の生成元 h 、および第 3 の生成元 f を選ぶ。このとき、 $g^{\alpha_1} h^{\alpha_2} f^{\alpha_3} = 1$ となる自明でない $\alpha_1, \alpha_2, \alpha_3$ を知らないように、 g, h, f を選ぶ。

同様に、 G_p から第 4 の生成元 G 、および第 5 の生成元 H を選ぶ。このとき、 $G^{\beta_1} H^{\beta_2} = 1$ となる自明でない β_1, β_2 を知らないように、 G, H を選ぶ。

また、任意のビット列を k ビットに変換する衝突困難ハッシュ関数 \mathcal{H}

を選ぶ。 k の値は 160 が推奨される。

そして、最後に、第 1 の素数 p 、第 2 の素数 q 、第 3 の素数 P 、第 1 の生成元 g 、第 2 の生成元 h 、第 3 の生成元 f 、第 4 の生成元 G 、第 5 の生成元 H 、および衝突困難ハッシュ関数 \mathcal{H}

を公開情報開示手段 101 に出力する。

次に、メンバー管理装置 4 は、離散対数鍵生成手段 401 により、メンバー登録手段 403 で用いる離散対数問題に基づく秘密鍵と公開鍵の対を作成する。この秘密鍵がメンバー登録秘密鍵であり、公開鍵がメンバー登録公開鍵である。

これらの作成において、第 1 の乱数生成器 404 は前処理手段 103 で選んだ第 2 の素数 q を位数とする有限体 Z_q からメンバー登録秘密鍵 v をランダムに選び、離散対数鍵生成手段 401 に入力する。次に、離散対数鍵生成手段 401 は、第 2 の生成元 h とメンバー登録秘密鍵 v から、メンバー登録公開鍵

$$y = h^v \bmod p$$

を計算する。すなわち、有限体上の乗法群の離散対数問題に基づく公開鍵と秘密鍵の計算においては、秘密鍵が、素数を位数とする有限体の任意の元であり、公開鍵が、その秘密鍵を離散対数とする値となるように、公開鍵および秘密鍵を選ぶこととなる。

最後に、メンバー登録公開鍵 y を公開情報開示手段 101 に出力し、メンバー登録秘密鍵 u をメンバー管理秘密情報記憶部 402 に厳重に保存する。

同様に、メンバー追跡装置 5 は、離散対数鍵生成手段 501 により、メンバー追跡手段 503 で用いる離散対数問題に基づく秘密鍵と公開鍵の対を作成する。

5 この秘密鍵がメンバー追跡秘密鍵であり、公開鍵がメンバー追跡公開鍵である。

これらの作成において、乱数生成器 504 は前処理手段 103 で作成した第 2 の素数 q を位数とする有限体 Z_q からメンバー追跡秘密鍵 ε をランダムに選び、離散対数鍵生成手段 501 に入力する。次に、離散対数鍵生成手段 501 は、第 1 の生成元 g とメンバー追跡秘密鍵 ε から、メンバー追跡公開鍵

10 $e = g^\varepsilon \bmod p$

を計算する。最後に、メンバー追跡公開鍵 e を公開情報開示手段 101 に出力し、メンバー追跡秘密鍵 ε をメンバー追跡秘密情報記憶部 502 に厳重に保存する。

以上の処理は、システムが動作を開始する際、もしくはシステムを初期化する際に行われる。

15 前処理および鍵生成の後、署名装置 2 はメンバー管理装置 4 との間で通信を行い、後に署名発行に使用する署名鍵とメンバー証明書を取得する。メンバー証明書は、署名装置 2 の第 5 の乱数生成器 214 が選んだ乱数を署名鍵とし、その署名鍵の変換データに対して、メンバー管理装置 4 が計算したメンバー管理秘密鍵を用いて、例えば、Nyberg と Rueppel による署名方式（“Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem,” Advances in Cryptology – EUROCRYPT ‘94, pp. 182–193）に従って作成した署名データである。

20 この署名データは Nyberg–Rueppel 署名と称される。このメンバー証明書は第 1 の要素および第 2 の要素で構成される。

25 以下、メンバー証明書の発行を行うメンバー登録手段 403 および登録手段 213 の動作の例を示す。

図 10 は、第 1 の実施形態によるグループ署名システムのメンバー登録時の動作を示すフローチャートである。

図10を参照すると、署名装置2の登録手段213は、まずステップA101で、第5の乱数生成器214で生成された、第2の素数 q を位数とする有限体 Z_q のいずれかの元 σ を署名装置2の署名鍵として受け取る。

次に、ステップA102で、署名鍵 σ の変換データとして

$$I_U = g^\sigma \bmod p$$

を計算する。

また、ステップA103で、署名鍵 σ が第1の生成元 g に関する署名鍵の変換データ I_U の離散対数であることの知識署名データ spk_U を計算する。知識署名データ spk_U は、Schnorrの“Efficient Signature Generation by Smart Cards” (Journal of Cryptology, 4, 3, pp. 161–174) に示された方法を用いて、次のように作成することができる。

有限体 Z_q から乱数 λ を選び、 (c, s) を次のように計算する。

$$c := \mathcal{H}(g \parallel I_U \parallel g^\lambda)$$

$$s := \lambda - c\sigma \bmod q$$

この計算で得られた

$$spk_U = (c, s)$$

が知識署名データとなる。

また、ステップA104で、署名鍵の変換データ I_U と知識署名データ spk_U を署名装置2が正しく作成したことを示す本人確認データを作成する。このデータには、署名鍵の変換データと知識署名データとの連結データに対するデジタル署名などを使用できる。

デジタル署名関数 Sig_U を用いる場合、本人確認データは

$$S_U = Sig_U(I_U \parallel spk_U)$$

となる。デジタル署名関数 Sig_U には、DSA署名やRSA署名などの署名アルゴリズムを使用することができる。

そして、署名装置2は変換データ I_U 、知識署名データ spk_U 、本人確認データ S_U をメンバー管理装置4に送信する。

メンバー管理装置 4 は、知識署名データ $s p k_U$ と本人確認データ S_U が正しいか否かを検証する（ステップ A 1 0 5）。知識署名データ $s p k_U$ の正しさは次の等式が成り立つ否かを確認することにより検証できる。

$$c = \mathcal{H}(g \| I_U \| I_U^c g^d)$$

5 一方、デジタル署名 S_U の正しさは、 $S i g_U$ に対応するデジタル署名検証関数 $V e r_U$ を用いて、

$$V e r_U (S_U, I_U \| s p k_U) = 1$$

が成り立つか否かを確認することにより検証できる。

10 両者ともが検証を通過したら処理が継続される。いずれか 1 つでも検証を通過できなければ、処理が中断される。

検証を通過した後、メンバー管理装置 4 のメンバー登録手段 4 0 3 は、ランダムに選んだ第 2 の素数 q を位数とする有限体 $Z q$ の元 ρ を第 2 の乱数生成器 4 0 5 から受け取る（ステップ A 1 0 6）。

15 次に、ステップ A 1 0 7 で、メンバー登録手段 4 0 3 は、受け取った乱数 ρ とメンバー管理秘密情報記憶部 4 0 2 に記憶されたメンバー管理秘密鍵 v と公開情報開示手段 1 0 1 に開示された第 2 の生成元 h とを使って、メンバー証明書 (r, ξ) を次のように計算する。

$$r := I_U h^{\rho} \bmod p$$

$$\xi := \rho - r v \bmod q$$

20 そして、メンバー管理装置 4 は計算で得たメンバー証明書 (r, ξ) を署名装置 2 に送信する。

ステップ A 1 0 8 において、署名装置 2 は受け取ったメンバー証明書 (r, ξ) が正しく作られているか否かを検証する。この検証は、次の等式が成り立つか否かを確認することにより行う。

$$r = y^r g^{\sigma} h^{\xi}$$

25 検証を通過したら、署名装置 2 は、メンバー管理装置 4 にメンバー証明書を確認できた旨を通知する（ステップ A 1 0 9）。そして署名装置 2 は、署名鍵 σ を秘密情報記憶部 2 1 1 に保存し、メンバー証明書 (r, ξ) をメンバー情報記憶

部 2 1 2 に保存する（ステップ A 1 1 0）。

また、メンバー管理装置 4 は、ステップ A 1 0 9 で通知された検証成功通知を受けとると、署名装置 2 を示すメンバーリストとして、署名鍵の変換データ I_U 、知識署名データ $s p k_U$ 、署名装置 2 に送信したメンバー証明書 (r, ξ) 、および本人確認データ S_U をメンバー情報開示手段 1 0 2 に出力する（ステップ A 1 1 1）。この登録処理は署名装置毎に行う。

メンバー証明書および署名鍵の作成が済んだ署名装置 2 は、メッセージ入力手段 2 0 9 から入力されたグループ署名を施すべき電子文書メッセージ m に対し、グループ署名を次のように作成する。

図 1 1 は、第 1 の実施形態による署名装置のグループ署名作成時の動作を示すフローチャートである。

図 1 1 を参照すると、ステップ A 2 0 1 で、第 1 の乱数生成器 2 0 1 が有限体 Z_q から第 1 の乱数 τ を生成し、第 2 の乱数生成器 2 0 2 が有限体 Z_q から第 2 の乱数 ω を生成し、第 3 の乱数生成器 2 0 3 が有限体 Z_p から第 3 の乱数 a を生成する。

次に、ステップ A 2 0 2 で、暗号化データ作成手段 2 0 5 は、第 1 の乱数 τ とメンバー証明書の第 1 の要素 r とメンバー追跡公開鍵 e を入力として、

$$g' := g^{\tau} \bmod p$$

$$e' := r^{-1} e^{\tau} \bmod p$$

を計算する。そして、この (g', e') を、メンバー証明書の第 1 の要素 r の暗号化データと呼ぶ。

次に、ステップ A 2 0 3 で、第 1 の変換データ作成手段 2 0 6 は、第 2 の乱数 ω とメンバー証明書の第 1 の要素 r を入力として、

$$h' := y^{\tau} f^{\omega} \bmod p$$

を計算する。この h' をメンバー証明書の第 1 の要素 r の第 1 の変換データと呼ぶ。

同様に、ステップ A 2 0 4 で、第 2 の変換データ作成手段 2 0 7 は、第 3 の乱数 a とメンバー証明書の第 1 の要素 r を入力として、

$$J := G^{\tau} H^a \bmod P$$

を計算する。この J をメンバー証明書第 1 の要素 r の第 2 の変換データと呼ぶ。

これらの暗号化および変換データは乱数を入力として作成しているので、変換データが公開されても、メンバー証明書第 1 の要素 r に関する情報は一切知られることがない。

5 これらの処理により、メンバー証明書第 1 の要素 r は、乱数を用いて秘匿されたことになる。

次に、ステップ A 2 0 5 で、知識署名作成手段 2 0 8 が知識署名データを作成する。

10 知識署名データは、メッセージ m を入力として、第 1 の変換データ h' および第 2 の変換データ J がメンバー証明書第 1 の要素 r の正しい変換であり、かつ h' と J が共に同じメンバー証明書第 1 の要素 r を変換していること、メンバー証明書 (r, ξ) をメンバー管理装置 4 と通信して正しく取得したこと、およびメンバー証明書 (r, ξ) に対応する署名鍵 σ を知っていること、暗号化データ (g', e') がメンバー証明書第 1 の要素 r をメンバー追跡公開鍵 e で正しく暗号化したものであることを、メンバー証明書 (r, ξ)、署名鍵 σ、第 1
15 の乱数 τ、第 2 の乱数 ω、および第 3 の乱数 a に関する情報を漏らさずに証明することのできるデータである。

本実施形態では、知識署名データは、等式

$$\left\{ \begin{array}{l} g' = g^{\tau} \bmod p \\ e' = r^{-1} e^{\tau} \bmod p \\ h' = y^{\tau} f^{\omega} \bmod p \\ J = G^{\tau} H^a \bmod p \\ e' h' = f^{\omega} g^{-\sigma} h^{-\xi} e^{\tau} \bmod p \\ r \in [0, p-1] \end{array} \right.$$

20 を満たす (r, ξ, σ, τ, ω, a) を知っていることを、(r, ξ, σ, τ, ω, a) を明かさないうままで (すなわち、これらの情報を漏らすことなく)、証明する。

まず最初に、 $1 \leq j \leq k$ として、0 から $p-1$ の間から乱数 ϕ_{2j-1} を選ぶ。ま

た、

$$\phi_{2j} := \phi_{2j-1} - p$$

とおく。

そして、次に、

$$5 \quad r + \phi_{2j} \in [0, p-1]$$

が成り立つか否か確認する。このとき、

$$r + \phi_{2j-1} \notin [0, p-1] \text{ かつ } r + \phi_{2j} \in [0, p-1]$$

であれば、 ϕ_{2j-1} と ϕ_{2j} を交換し、

$$10 \quad r + \phi_{2j-1} \in [0, p-1]$$

となるように値を置き換える。

また、有限体 Z_q から乱数 ψ_{2j-1} , ψ_{2j} を、有限体 Z_p から乱数 η_{2j-1} , η_{2j} をランダムに選ぶ。これらの乱数を用いて、 $1 \leq j \leq k$ について次の値を計算する。

$$V_j := y^{\phi_{2j-1}} f^{\psi_{2j-1}} \| y^{\phi_{2j}} f^{\psi_{2j}} \| G^{\phi_{2j-1}} H^{\eta_{2j-1}} \| G^{\phi_{2j}} H^{\eta_{2j}}$$

15 次に、有限体 Z_q の元 t_1 , t_2 , t_3 , t_4 , t_5 をランダムに選び、それらを用いて、

$$T_1 := y^{t_1} f^{t_2} \bmod p$$

$$T_2 := f^{t_2} g^{-t_3} h^{-t_4} e^{t_5} \bmod p$$

$$T_3 := g^{t_5} \bmod p$$

を計算する。

また、 $1 \leq j \leq k$ について、有限体 Z_q から乱数 r_j を、有限体 Z_p から乱数 u_j を選び、

20

$$e_j := e^{r_j} \bmod p$$

を計算する。また、

$$g_j := g^{\gamma_j} \bmod p$$

$$J_j := G^{e_j} H^{u_j} \bmod P$$

を計算する。

そして、これらの値から知識署名データ

$$c := \mathcal{H}(g \| h \| f \| G \| H \| y \| e \| V_1 \| \cdots \| V_k \| T_1 \| T_2 \| T_3 \| g_1 \| \cdots \| g_k \| J_1 \| \cdots \| J_k \| m)$$

5 、および、 $c[j] = 0$ のとき

$$v_{6j-5} := \phi_{2j-1}$$

$$v_{6j-4} := \phi_{2j}$$

$$v_{6j-3} := \psi_{2j-1}$$

$$v_{6j-2} := \psi_{2j}$$

$$v_{6j-1} := \eta_{2j-1}$$

$$v_{6j} := \eta_{2j}$$

$$w_j := \gamma_j \bmod q$$

$$z_j := u_j \bmod p$$

、 $c[j] = 1$ のとき、

$$v_{6j-5} := rU + \phi_{2j-1}$$

$$v_{6j-4} := y^{\phi_{2j}} f^{\psi_{2j}}$$

$$v_{6j-3} := \omega + \psi_{2j-1}$$

$$v_{6j-2} := \psi_0 \in_U Z_q$$

$$v_{6j-1} := a + \eta_{2j-1}$$

$$v_{6j} := G^{\phi_{2j}} H^{\eta_{2j}}$$

$$w_j := \gamma_j - \tau \bmod q$$

$$z_j := u_j - ae_j r U^{-1} \bmod p$$

を計算する。ここで、 $c[j]$ は c の j 番目のビットの値を表す。

10 c および $(v_1, v_2, v_3, v_4, v_5, v_6, \dots, v_{6k-5}, v_{6k-4}, v_{6k-3}, v_{6k-2}, v_{6k-1}, v_{6k})$ の部分は、メンバー証明書の第1の要素 r を第2の乱数 ω および第3の乱数 a を用いて正しく変換していることと、2つの式で変換されている r が同じ r であることを証明する。つまり、

$$h' = y^r f^{\omega} \bmod p \text{ かつ } J = G^r H^a \bmod P \text{ かつ } r \in [0, p-1]$$

であることを示している。

c および (s₁, s₂, s₃, s₄, s₅) の部分は、メンバー証明書 (r, ξ) と署名鍵 ω を正しく作成したことを証明する。つまり、

$$e' h' = f^{\omega} g^{-\sigma} h^{\xi} e^r \bmod p \text{ かつ } h' = y^r f^{\omega} \bmod p \text{ かつ } g' = g^r \bmod p$$

5

であることを示している。

c および (w₁, ..., w_k, z₁, ..., z_k) の部分は、第2の変換データ J で変換されたメンバー証明書の第1の要素 r を暗号化データ (g', e') で正しく暗号化していることを証明する。つまり、

$$J = G^r H^a \bmod P \text{ かつ } g' = g^r \bmod p \text{ かつ } e' = r^{-1} e^r \bmod p$$

10

であることを示している。

最後に、署名出力手段 210 は、ステップ A206 で、暗号化データ (g', e')、第1の変換データ h'、第2の変換データ J、知識署名データ (c, v₁, v₂, v₃, v₄, v₅, v₆, ..., v_{6k-5}, v_{6k-4}, v_{6k-3}, v_{6k-2}, v_{6k-1}, v_{6k}, s₁, s₂, s₃, s₄, s₅, w₁, ..., w_k, z₁, ..., z_k) をグループ署名として出力する。

15

検証手段 301 は、与えられたグループ署名が正しく作られたものであるか否かを確認する。この検証は、グループ署名に含まれる知識署名データを検証することにより行う。

20

知識署名データの検証では、与えられたグループ署名の署名者が、メンバー登録手段 403 と通信することで作成したメンバー証明書 (r, ξ) および署名鍵 σ を正しく所有しているか否かを確認することができる。しかし、グループ署名データ内では、メンバー証明書 (r, ξ) および署名鍵 σ は乱数を用いて秘匿されているので、登録された署名装置のうちどの装置が署名を作成したかの情報は検証を通じて得ることができない。

25

本実施の形態では、知識署名データの検証は、次の等式が成り立つか否かの確

認により行う。

$$c = \mathcal{H}(g \| h \| f \| G \| H \| y \| e \| V_1' \| \cdots \| V_k' \| T_1' \| T_2' \| T_3' \| g_1' \| \cdots \| g_k' \| J_1' \| \cdots \| J_k' \| m)$$

ここで、

$$V_j' = \begin{cases} y^{v_{6j-5}} f^{v_{6j-3}} \| y^{v_{6j-4}} f^{v_{6j-2}} \| & c[j] = 0 \\ G^{v_{6j-5}} H^{v_{6j-1}} \| G^{v_{6j-4}} H^{v_{6j}} & \\ y^{v_{6j-5}} f^{v_{6j-3}} / h' \| v_{6j-4} \| & c[j] = 1 \\ G^{v_{6j-5}} H^{v_{6j-1}} / J \| v_{6j} & \end{cases}$$

$$T_1' = h'^c y^{s_1} f^{s_2}$$

$$T_2' = (e' h')^c f^{s_2} g^{-s_3} h^{-s_4} e^{s_5}$$

$$T_3' = g'^c g^{s_5}$$

$$g_j' = g'^{c[j]} g^{w_j} \bmod p$$

$$J_j' = \begin{cases} G^{\bar{e}_j'} H^{z_j} \bmod P & c[j] = 0 \\ J^{\bar{e}_j'} H^{z_j} \bmod P & c[j] = 1 \end{cases}$$

(where $\bar{e}_j' := e'^{c[j]} e^{w_j} \bmod p$)

5 である。

そして、知識署名データが正しいことが確認できたら、そのグループ署名を受理する。知識署名データが正しくなければ、署名を不受理とする。

メンバー追跡装置 5 では、メンバー追跡手段 5 0 3 が、検証装置 3 0 1 で受理されたグループ署名の実際の署名者を特定する。

10 まず、メンバー追跡秘密情報記憶部 5 0 2 に記憶されたメンバー追跡秘密鍵 ε を用いて、

$$\bar{r} := g'^{\varepsilon} / e' \bmod p$$

を計算し、グループ署名の暗号化データ (g' , e') から与えられた署名の署名者を表すメンバー証明書第 1 の要素

15 \bar{r}

を復号する。また、それと同時に、メンバー追跡秘密情報記憶部 5 0 2 に記憶されたメンバー追跡秘密鍵 ε を用いて、復号結果

\bar{r}

が暗号化データ (g', e') をメンバー追跡秘密鍵 ε を用いて正しく復号した結果であることの証明データを次のように作成する。

有限体 Z_q から乱数 δ を選び、

$$c := \mathcal{H}(g' \| e' \| \bar{r}^{-1} e' \| g'^{\delta})$$

$$s := \delta - c\varepsilon \bmod q$$

5

を計算する。この (c, s) が証明データとなる。この証明データによる証明で、メンバー追跡装置 5 がグループ署名から

\bar{r}

を正しく復号したことが保証されることとなる。

10

次に、メンバー情報開示手段 102 に開示されたメンバーリスト $\{<I_U, s p k_U, r, \xi, S_U>\}$ の中から、復号されたメンバー証明書の第 1 の要素

\bar{r}

と同一のメンバー証明書の第 1 の要素 r を含むメンバーリスト $(I_U, s p k_U, r, \xi, S_U)$ を検索する。検索できたら、合致したメンバーリストに対応する署名装置を、そのグループ署名の署名者であると特定する。

15

なお、本実施形態において、メンバー管理装置 4 とメンバー追跡装置 5 はグループ管理装置 1 の中に含まれることとしてもよい。また、演算に用いている有限体上の乗法群の代わりに、楕円曲線上の有限群を用いることとしてもよい。

20

以上説明したように、本実施形態によれば、暗号化データ作成手段 205、第 1 の変換データ作成手段 206、および第 2 の変換データ作成手段 207 にて、メンバー証明書に関する情報を、後にグループ署名の要素として開示されることのない乱数を用いて秘匿しているので、メンバー追跡に必要な秘密情報を持たない装置はグループ署名データから署名者に関する情報を得ることができず、安全確実なグループ署名を提供することができ、また、メンバー管理装置 4 が署名者を特定することができず、グループ管理装置の機能をメンバー管理装置 4 とメンバー追跡装置 5 に安全に分割することができる。

25

次に、本発明の第 2 の実施形態について図面を参照して詳細に説明する。

図 1 2 は、第 2 の実施形態のグループ署名システムの構成例を示すブロック図である。図 1 2 を参照すると、第 2 の実施形態のグループ署名システムは、グループ管理装置 1、署名装置 2、検証装置 3、第 1 ～ 3 のメンバーサブ管理装置 6 ～ 8、第 1 ～ 3 のメンバーサブ追跡装置 9 ～ 1 1 を有する。

5 本実施形態では、メンバーサブ管理装置およびメンバーサブ追跡装置をそれぞれ 3 つずつに分散する場合を例に説明するが、各装置の数に制限はない。第 1 ～ 3 のメンバーサブ管理装置 6 ～ 8 の間、および第 1 ～ 3 のメンバーサブ追跡装置間 9 ～ 1 1 の間は、相互にブロードキャストチャネルで結ばれている。そして、第 1 ～ 3 のメンバーサブ管理装置 6 ～ 8 は、機能を分散して、グループメンバー
10 の登録処理を行う。第 1 ～ 3 のメンバーサブ追跡装置 9 ～ 1 1 は、機能を分散して、グループ署名から署名を作成したメンバーを特定する。

グループ管理装置 1 は、第 1 の実施形態と同様の構成を有し、システム全体で使用する公開情報を開示する。署名装置 2 は第 1 の実施形態と同様の構成を有している。また、検証装置 3 は第 1 の実施形態と同様の構成を有している。

15 第 1 ～ 3 のメンバーサブ管理装置 6 ～ 8 の各々は、分散離散対数鍵生成手段 6 0 1、7 0 1、8 0 1、分散登録秘密情報記憶部 6 0 2、7 0 2、8 0 2、分散メンバー登録手段 6 0 3、7 0 3、8 0 3、および乱数生成器 6 0 4、7 0 4、8 0 4 を有している。以下簡単のため、メンバーサブ管理装置 6 について説明する。

20 分散離散対数鍵生成手段 6 0 1 は、他のメンバーサブ管理装置と通信を行いながら、分散メンバーサブ管理手段 6 0 3 で用いる分散登録秘密鍵を生成し、分散登録秘密情報記憶部 6 0 2 に出力する。

分散登録秘密情報記憶部 6 0 2 は、分散離散対数鍵生成手段 6 0 1 で生成した分散登録秘密鍵を記憶する。

25 分散メンバー登録手段 6 0 3 は、署名装置 2 と通信を行いながら、その署名装置 2 に対してメンバー証明書を発行する。ただし、分散メンバー登録手段 6 0 3 が出力するメンバー証明書は、単体ではメンバー証明書としての機能を持たない。署名装置 2 は各メンバー管理装置から受け取ったメンバー証明書から後に使用するメンバー証明書を計算することができる。

乱数生成器 604 は、分散離散対数鍵生成手段 601 および分散メンバー登録手段 603 で使用する乱数を生成する。

第 1、第 2、第 3 のメンバーサブ追跡装置 9、10、11 の各々は、分散離散対数鍵生成手段 901、1001、1101、分散追跡秘密情報記憶部 902、
5 1002、1102、分散メンバー追跡手段 903、1003、1103、乱数生成器 904、1004、1104 を有している。以下簡単のため、メンバーサブ追跡装置 9 について説明する。

分散離散対数鍵生成手段 901 は、他のメンバーサブ追跡装置と通信を行いながら、分散メンバー追跡手段 903 で用いる分散追跡秘密鍵を生成し、分散追跡
10 秘密情報記憶部 902 に出力する。

分散追跡秘密情報記憶部 902 は、分散離散対数鍵生成装置 901 で生成した分散追跡秘密鍵を記憶する。

分散メンバー追跡手段 903 は、他のメンバーサブ追跡装置と通信を行いながら、検証装置 3 の検証手段 301 で受理されたグループ署名と、分散追跡秘密情報記憶部 902 に記憶された分散追跡秘密鍵と、メンバー情報開示手段 102 で
15 開示されたメンバー情報とを入力として、グループ署名の署名者を特定し出力する。

乱数生成器 904 は、分散離散対数鍵生成手段 901 および分散メンバー追跡手段 903 で使用する乱数を生成する。

以下、第 2 の実施形態のグループ署名システムの詳細動作について説明する。

まず最初に前処理として、第 1 の実施形態と同様に、グループ管理装置 1 の前
処理手段 103 が公開情報
($p, q, P, g, h, f, G, H, \mathcal{H}$)

を生成し、それを公開情報開示手段 101 が開示する。

次に、第 1、第 2、第 3 のメンバーサブ管理装置 6、7、8 の分散離散対数鍵生成手段 601、701、801 の各々が、メンバー登録に用いる公開鍵と分散秘密鍵を作成し、分散秘密鍵を分散登録秘密情報記憶部 602、702、802
25 に記録する。分散秘密鍵は、単体では秘密鍵としての役割を果たさないが、3つ

のメンバーサブ管理装置 6、7、8 の全てが正しく動作することにより、第 1 の実施形態のメンバー登録秘密鍵を使った処理と同様の機能を果たす。

本実施形態では、一例として、Pedersen の “A Threshold Cryptosystem without a Trusted Party” (Advances in Cryptology—EUROCRYPT ‘91, pp. 522–526) に示された離散対数問題に基づく暗号系の分散秘密鍵生成方法に従った鍵生成手段を示す。

第 1、第 2、第 3 のメンバーサブ管理装置 6、7、8 の各々は、まず、 Z_q 上の 2 次の多項式をランダムに選ぶ。ここで、第 1 のメンバーサブ管理装置 6 は多項式 $f_1(z)$ を選ぶ。

$$f_1(z) = a_{10} + a_{11}z + a_{12}z^2 \bmod q$$

第 2、第 3 のメンバーサブ管理装置 7、8 も、それと同様に $f_2(z)$ 、 $f_3(z)$ をそれぞれ選ぶ。

第 1 のメンバーサブ管理装置 6 は、

$$H_{11} = h^{a_{11}} \bmod p, H_{12} = h^{a_{12}} \bmod p, H_{13} = h^{a_{13}} \bmod p$$

を第 2 のメンバーサブ管理装置 7 および第 3 のメンバーサブ管理装置 8 に送信する。

同様に、第 2 のメンバーサブ管理装置 7 は H_{21} 、 H_{22} 、 H_{23} を第 1 および第 3 のメンバーサブ管理装置 6、8 に送り、第 3 のメンバーサブ管理装置 8 は H_{31} 、 H_{32} 、 H_{33} を第 1 および第 2 のメンバーサブ管理装置 6、7 に送る。

ここで a_{10} 、 a_{20} 、 a_{30} をそれぞれ v_1 、 v_2 、 v_3 と表記すると、 v_1 、 v_2 、 v_3 がそれぞれのメンバーサブ管理装置 6、7、8 の分散登録秘密鍵となる。また、

$$y_1 = H_{10} = h^{v_1} \bmod p, y_2 = H_{20} = h^{v_2} \bmod p, y_3 = H_{30} = h^{v_3} \bmod p$$

が公開情報開示手段 101 に出力される。

そして、第 1 のメンバーサブ管理装置 6 は

$$\bar{v}_{12} = f_1(2) \bmod q$$

を第 2 のメンバーサブ管理装置 7 に、

$$\bar{v}_{13} = f_1(3) \bmod q$$

を第 3 のメンバーサブ管理装置 8 に、他の装置に内容が知られないよう秘密に、
5 それぞれ送信する。

同様に、第 2 のメンバーサブ管理装置 7 は

$$\bar{v}_{21} = f_2(1) \bmod q$$

を第 1 のメンバーサブ管理装置 6 に、

$$\bar{v}_{23} = f_2(3) \bmod q$$

10 を第 3 のメンバーサブ管理装置 8 に、秘密に、送信する。また、第 3 のメンバーサブ管理装置 7 は

$$\bar{v}_{31} = f_3(1) \bmod q$$

を第 1 のメンバーサブ管理装置 6 に、

$$\bar{v}_{32} = f_3(2) \bmod q$$

15 を第 2 のメンバーサブ管理装置 7 に、秘密に、送信する。

これにより、第 1 のメンバーサブ管理装置 6 は、第 2 のメンバーサブ管理装置 7 から H_{21} , H_{32} , H_{23} および

$$\bar{v}_{21}$$

を、第 3 のメンバーサブ管理装置 8 から H_{31} , H_{32} , H_{33} および

20 \bar{v}_{31}

をそれぞれ受け取ることになる。

そして、第 1 のメンバーサブ管理装置 6 は他のメンバーサブ管理装置から受け
取った

$$\bar{v}_{21}$$

25 および

$$\bar{v}_{31}$$

を検証する。この検証は次の等式を満たすか否かを確認することにより行なわれる。

$$h^{\bar{v}_{21}} = (H_{21})^{1^1} \cdot (H_{22})^{1^2} \cdot (H_{23})^{1^3} \bmod p$$

$$h^{\bar{v}_{31}} = (H_{31})^{1^1} \cdot (H_{32})^{1^2} \cdot (H_{33})^{1^3} \bmod p$$

メンバーサブ管理装置の各々は、この検証に失敗すると、その値の送り元のメンバーサブ管理装置に対して、検証失敗の旨を通知する。他の2つのメンバーサブ管理装置の双方から検証失敗の通知を受けたメンバーサブ管理装置は管理者としての資格を失う。

また、他のメンバーサブ管理装置のいずれか一方のみから検証失敗の通知を受けた場合、例えば、第1のメンバーサブ管理装置6のみが第2のメンバーサブ管理装置7の検証に失敗した場合には、第2のメンバーサブ管理装置7は、検証式を満たす

\bar{v}_{21}

を再び第1のメンバーサブ管理装置6に送信する。この

\bar{v}_{21}

が第1のメンバーサブ管理装置6にて検証式を満たさないとき、第2のメンバーサブ管理装置7は管理者としての資格を失う。第2のメンバーサブ管理装置7が資格を失った場合、 $v_2 = 0$ 、 $y_2 = 1$ として、それ以降の処理を続ける。

メンバーサブ管理装置に共通のメンバー登録公開鍵 y は、

$$y = y_1 \cdot y_2 \cdot y_3 \cdot \bmod p$$

として計算する。つまり、各メンバーサブ管理装置6、7、8は、自身の分散登録秘密鍵が、素数を位数とする有限体の元を求めるための複数に分散された値のうちの自身に割り当てる1つであり、かつ、登録公開鍵が、その複数の分散登録秘密鍵から定まる元を離散対数とする値となるように、登録公開鍵と分散登録秘密鍵を求める。このとき、登録公開鍵は有限体上の乗法群の元となる。

そして、公開鍵 y をグループ管理装置1の公開情報開示手段101に開示させ、第1、第2、第3のメンバーサブ管理装置6、7、8の各々は、 v_1 、 v_2 、 v_3 を分散登録秘密鍵として、それぞれの分散登録秘密情報記憶部602、702、802に記憶する。

同様に、第1、第2、第3のメンバーサブ追跡装置9、10、11の分散離散

対数鍵生成手段 9 0 1、1 0 0 1、1 1 0 1 は、メンバー追跡に用いる公開鍵と分散秘密鍵を作成する。そして、分散秘密鍵をメンバー追跡秘密鍵として、分散追跡秘密情報記憶部 9 0 2、1 0 0 2、1 1 0 2 に記憶する。また、公開鍵をメンバー追跡公開鍵としてグループ管理装置 1 の公開情報開示手段 1 0 1 に開示させる。ここでメンバー追跡公開鍵は e と表し、それぞれのメンバーサブ追跡装置が持つ秘密鍵を ε_1 、 ε_2 、 ε_3 と表す。

前処理および鍵生成の後、署名装置 2 は第 1、第 2、第 3 のメンバーサブ管理装置 6、7、8 との間で通信を行い、第 1 の実施形態と同様に、メンバー証明書 (r 、 ξ) および秘密鍵 σ を取得する。

署名装置 2 の登録手段 2 1 3 は、図 1 0 のステップ A 1 0 1 から A 1 0 4 と同様の動作により、第 5 の乱数生成器 2 1 4 で生成した有限体 Z_q から選んだ乱数 σ を署名鍵とし、署名鍵の変換データ I_U 、知識署名データ s_{pk_U} 、および本人確認データ S_U を作成する。そして、署名装置 2 は変換データ I_U 、知識署名データ s_{pk_U} 、および本人確認データ S_U を第 1、第 2、第 3 のメンバーサブ管理装置 6、7、8 のすべてに送信する。

変換データ I_U 、知識署名データ s_{pk_U} 、および本人確認データ S_U を受け取った第 1、第 2、第 3 のメンバーサブ管理装置 6、7、8 はそれぞれ、図 1 0 のステップ A 1 0 5 と同様に、知識署名データ s_{pk_U} と本人確認データ S_U が正しいかどうか検証する。

それらの双方が検証を通過したら以降の処理を続ける。検証を通過しなければ処理が中断される。

検証の後、第 1、第 2、第 3 のメンバーサブ管理装置 6、7、8 は、分散メンバー管理秘密鍵の生成と同様に、有限体 Z_q の元である乱数 k に対応する分散情報 k_1 、 k_2 、 k_3 を計算する。また、第 1 のメンバーサブ管理装置 6 は

$$t_1 = h^{k_1} \bmod p$$

を、第 2 のメンバーサブ管理装置 7 は

$$t_2 = h^{k_2} \bmod p$$

を、第3のメンバーサブ管理装置8は

$$t_3 = h^{k_3} \bmod p$$

を公開情報開示手段101に出力する。また、

$$t = t_1 \cdot t_2 \cdot t_3 \bmod p$$

5 も公開情報開示手段101にて開示される。

次に、第1、第2、第3のメンバーサブ管理装置6、7、8は、公開情報tを用いて、メンバー証明書の第1の要素

$$r := I_U h^t \bmod p$$

10 を計算する。rは公開情報tを入力として計算されるため、すべてのメンバーサブ管理者で等しい値が得られる。また、分散生成した乱数 k_1 、 k_2 、 k_3 と分散登録秘密情報記憶部602、702、802に記憶された分散秘密鍵 u_1 、 u_2 、 u_3 を用いて、第1、第2、第3のメンバーサブ管理装置6、7、8の各々は
 $\xi_1 = k_1 - ru_1 \bmod q$ 、 $\xi_2 = k_2 - ru_2 \bmod q$ 、および $\xi_3 = k_3 - ru_3 \bmod q$

15

の各々を計算する。そして、第1のメンバーサブ管理装置6は (r, ξ_1) を、第2のメンバーサブ管理装置7は (r, ξ_2) を、第3のメンバーサブ管理装置8は (r, ξ_3) を署名装置2にそれぞれ送信する。

署名装置2は、受け取ったメンバー証明書 (r, ξ_1) 、 (r, ξ_2) 、 (r, ξ_3) が正しく作られているか否かを、

20

$$h^{\xi_1} = t_1 y_1^{-r} \bmod p, h^{\xi_2} = t_2 y_2^{-r} \bmod p, \text{ および } h^{\xi_3} = t_3 y_3^{-r} \bmod p$$

が満たされるか否かを確認することにより検証する。この検証を通過したら、署名装置2は第1、第2、第3のメンバーサブ管理装置6、7、8にメンバー証明書を
 確認できた旨を通知する。その後、署名装置2は、第1、第2、第3のメン
 25 ーサブ管理装置6、7、8から受け取った全てのメンバー証明書の第2の要素
 を入力として、

$$\xi = \xi_1 + \dots + \xi_n$$

を計算する。そして署名装置 2 は、 (r, ξ) をメンバー証明書としてメンバー情報記憶部 212 に記憶する。また、署名鍵 σ を秘密情報記憶部 211 に記憶する。

またメンバー管理装置 4 は、検証成功の通知を受けると、署名装置 2 を示すメンバーリストとして、署名装置 2 に送信したメンバー証明書、署名装置 2 から受け取った署名鍵の変換データ、知識署名データ、本人確認データをメンバー情報開示手段 102 に出力する。

本実施形態では、署名装置 2 における署名作成、検証装置 3 における署名検証は第 1 の実施形態と同様に行われる。

第 1、第 2、第 3 のメンバーサブ追跡装置 9、10、11 のメンバー追跡装置 903、1003、1103 は次のように動作する。

第 1、第 2、第 3 のメンバーサブ追跡装置 9、10、11 は、まず、与えられたグループ署名に含まれる暗号化データ (g', e') の復号を行う。各メンバーサブ追跡装置 9、10、11 の各々は、分散追跡秘密情報記憶部 902、1002、1102 の各々に記憶された分散追跡秘密鍵 $\varepsilon_1, \varepsilon_2, \varepsilon_3$ を用いて、

$$g'_1 := g'^{\varepsilon_1} \bmod p, g'_2 := g'^{\varepsilon_2} \bmod p, g'_3 := g'^{\varepsilon_3} \bmod p$$

をそれぞれ計算する。これらを用いて、

$$\bar{r} := g'^{\varepsilon} / e' = (g')^{\varepsilon_1 + \varepsilon_2 + \varepsilon_3} / e' = (g'_1 \cdot g'_2 \cdot g'_3) / e' \bmod p$$

を計算すると、与えられたグループ署名の署名者に該当するメンバー証明書の復号結果

\bar{r}

を得ることができる。そして、第 1 の実施形態と同様に、メンバー情報開示手段 102 に開示されたメンバーリスト $\{<I_U, spk_U, r, \xi, S_U>\}$ の中から、復号されたメンバー証明書の第 1 の要素

\bar{r}

と同一の、メンバー証明書の第 1 の要素 r を含むメンバーリスト $(I_U, spk_U, r, \xi, S_U)$ を検索し、合致したメンバーリストに対応する署名装置 2 を署名者と特定する。

なお、本実施形態では、メンバーサブ管理装置およびメンバーサブ追跡装置が3つずつであり、これら全ての装置が正しく動作したときに正しい処理が行われる。これを一般化して、メンバーサブ管理装置およびメンバーサブ追跡装置をn個ずつとした場合、

5 $t < n / 2$

とにおいて、鍵生成の際に第iのメンバーサブ管理装置もしくはメンバーサブ追跡装置が選ぶ多項式を

$$f_i(z) = a_{i0} + a_{i1}z + \dots + a_{it}z^t \bmod q$$

10 とすれば、t個以上のメンバーサブ管理装置もしくはメンバーサブ追跡装置が正しく動作したときにのみ、正しくメンバー登録および追跡処理を行うことができるものとなる。

15 以上説明したように、本実施形態によれば、メンバー管理装置の機能は複数のメンバーサブ管理装置に分散され、複数のメンバーサブ管理装置がメンバー証明書を計算するために使用する秘密鍵は、離散対数問題に基づく暗号系から選ばれるため、メンバーサブ管理装置の分散秘密鍵生成と分散メンバー登録処理の計算量が低減され、メンバーサブ管理装置の各々の負荷を低減することができる。

20 また、本実施形態によれば、メンバー追跡装置の機能は複数のメンバーサブ追跡装置に分散され、複数のメンバーサブ追跡装置が署名者の特定に用いる秘密鍵は、離散対数問題に基づく暗号系から選ばれるため、メンバーサブ管理装置の分散秘密鍵生成と署名者特定の分散した処理の計算量が低減され、メンバーサブ追跡装置の各々の負荷を低減することができる。

25 本発明によれば、署名装置が、メンバー証明書に関する情報を、グループ署名の要素として開示されない乱数を用いて秘匿するため、メンバー追跡に必要な秘密鍵を持たない装置はそれを解読できないので、特別な装置（メンバー追跡装置）以外はグループ署名から署名者を特定することができず、安全確実なグループ署名を提供することができる。また、メンバー登録を管理する機能と、グループ署名の署名者を特定する機能をグループ管理装置から分割する場合に、安全に分割することができる。また、メンバー管理装置の機能は複数のメンバーサブ管理装

5 置に分散され、複数のメンバーサブ管理装置がメンバー証明書を計算するために使用する秘密鍵は、離散対数問題に基づく暗号系から選ばれるため、メンバーサブ管理装置の分散秘密鍵生成と分散メンバー登録処理の計算量が低減され、メンバーサブ管理装置の各々の負荷を低減することができる。また、メンバー追跡装置の機能は複数のメンバーサブ追跡装置に分散され、複数のメンバーサブ追跡装置が署名者の特定に用いる秘密鍵は、離散対数問題に基づく暗号系から選ばれるため、メンバーサブ管理装置の分散秘密鍵生成と署名者特定の分散した処理の計算量が低減され、メンバーサブ追跡装置の各々の負荷を低減することができる。

請求の範囲

1. 署名者がグループに登録されたメンバーであることを証明することのできるグループ署名を作成し、グループ署名の署名者が前記グループのメンバーであるか否か確認するグループ署名システムであって、

システム内で共通に利用する公開情報を他の装置から参照可能に開示するグループ管理装置と、

第1の要素及び第2の要素を含むメンバー証明書の前記第1の要素を第1の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成し、前記第1の要素を第2の乱数および前記公開情報を用いて変換して第1の変換データを作成し、前記第1の要素を第3の乱数および前記公開情報を用いて変換して第2の変換データを作成し、署名を付加すべきメッセージ、第4の乱数、前記暗号化データ、前記第1の変換データ、前記第2の変換データ、署名の作成に用いる秘密鍵である署名鍵、前記第1の要素、および前記第2の要素から、知識署名データを作成し、前記暗号化データ、前記第1の変換データ、前記第2の変換データ、および前記知識署名データをグループ署名として前記メッセージと共に出力する署名装置と、

メッセージおよびグループ署名と、前記グループ管理装置にて開示されている前記公開情報とから、前記グループ署名が、前記グループに登録されているいずれかのメンバーのメンバー証明書に含まれる第1の要素および第2の要素と前記署名鍵を用いて作成されたものか否かを検証する検証装置とを有するグループ署名システム。

2. 前記署名装置は、前記暗号化データ、前記第1の変換データ、および前記第2の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第1の要素、前記第2の要素、および前記署名鍵に関する情報を知られることのないデータとして、前記知識署名データを作成し、

前記検証装置は、前記グループ署名が、前記グループに登録されているいずれかのメンバーのメンバー証明書に含まれる第1の要素および第2の要素と前記署

名鍵を用いて作成されたものか否かを、前記第1の要素、前記第2の要素、および前記署名鍵に関する情報を用いることなく、検証することを特徴とする請求項1に記載のグループ署名システム。

5 3. 新たなメンバーを前記グループに登録するとき、素数を位数とする有限体の元となるようにメンバー登録秘密鍵を選び、前記メンバー登録秘密鍵を離散対数とし、有限体上の乗法群の元であるメンバー登録公開鍵を前記メンバー登録秘密鍵から求め、前記メンバー登録公開鍵を公開情報として前記グループ管理装置に通知し、前記メンバー登録秘密鍵を自身で記憶すると共に、該メンバー登録秘密鍵を用いてメンバー証明書を作成し、前記署名装置に通知するメンバー管理装置をさらに有する、請求項1または請求項2に記載のグループ署名システム。

15 4. 前記メンバー証明書は、前記署名鍵を離散対数とする、前記署名鍵の変換データに対して前記メンバー登録秘密鍵を用いて作成したNyberg-Rueppel署名である、請求項3に記載のグループ署名システム。

20 5. 前記グループ管理装置は、前記公開情報に加えて、前記メンバー管理装置から通知された前記メンバー情報を他の装置から参照可能に開示する、請求項3または請求項4に記載のグループ署名システム。

25 6. 新たなメンバーを前記グループに登録するとき、素数を位数とする有限体の所定の元の、複数に分散された値のうちの1つを自身の分散メンバー登録秘密鍵として割り当て、前記分散メンバー登録秘密鍵を自身で記憶すると共に、前記元を離散対数とする値をメンバー登録公開鍵とする、複数のメンバーサブ管理装置をさらに有し、

前記署名装置は、複数の前記メンバーサブ管理装置と通信することによりメンバー証明書を取得し、

前記グループ管理装置は、前記メンバー登録公開鍵を取得する、請求項1または請求項2に記載のグループ署名システム。

7. 素数を位数とする有限体の元となるようにメンバー追跡秘密鍵を選び、前記メンバー追跡秘密鍵を離散対数とし、有限体上の乗法群の元であるメンバー追跡公開鍵を前記メンバー追跡秘密鍵から求め、前記メンバー追跡公開鍵を前記公開情報として前記グループ管理装置に通知し、前記メンバー追跡秘密鍵を自身で記憶しておき、グループ署名の署名者を特定するとき、前記グループ署名に含まれている暗号化データを前記メンバー追跡秘密鍵を用いて復号し、復号結果と前記グループ管理装置にて開示されているいずれかの前記メンバー証明書の第1の要素とが一致すれば該メンバー証明書のメンバーを署名者と特定するメンバー追跡装置をさらに有し、

前記グループ管理装置は前記メンバー証明書を前記メンバー情報として開示しており、

前記署名装置は前記第1の要素を暗号化して前記暗号化データを作成するとき前記公開情報として前記メンバー追跡公開鍵を用いる、請求項1から請求項6のいずれか1項に記載のグループ署名システム。

8. 自身の分散メンバー追跡秘密鍵が、素数を位数とする有限体の元の複数の分散された値のうちの自身に割り当てる1つであり、メンバー追跡公開鍵が、前記有限体の元を離散対数とし、有限体上の乗法群の元となるように、前記分散メンバー追跡秘密鍵を求め、前記分散メンバー追跡秘密鍵を自身で記憶する複数のメンバーサブ追跡装置をさらに有し、

前記署名装置は前記第1の要素を暗号化して前記暗号化データを作成するとき前記公開情報として前記メンバー追跡公開鍵を用い、

前記グループ管理装置は前記メンバー証明書を前記メンバー情報として開示しており、

グループ署名の署名者を特定するとき、前記メンバーサブ追跡装置の各々が前記グループ署名に含まれている暗号化データに対して自身の前記分散メンバー追跡秘密鍵を用いて所定の計算をした結果から求まる復号結果と、前記グループ管理装置にて開示されているいずれかの前記メンバー証明書の第1の要素とが一致

すれば該メンバー証明書のメンバーを署名者と特定する、請求項 1 から請求項 6 のいずれか 1 項に記載のグループ署名システム。

9. 前記有限体上の乗法群に代えて楕円曲線上の有限群を用いる、請求項 3、
5 6、7、8 のいずれか 1 項に記載のグループ署名システム。

10. グループ管理装置、署名装置、および検証装置を有するグループ署名システムにおいて、署名者がグループに登録されたメンバーであることを証明することのできるグループ署名を作成し、グループ署名の署名者が前記グループのメンバーであるか否か確認するためのグループ署名方法であって、
10

前記グループ管理装置において、

システム内で共通に利用する公開情報を他の装置から参照可能に開示するステップと、

前記署名装置において、

15 第 1 の要素および第 2 の要素を含むメンバー証明書を記憶するステップと、

前記第 1 の要素を第 1 の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成するステップと、

前記第 1 の要素を第 2 の乱数および前記公開情報を用いて変換して第 1 の変換データを作成するステップと、

20 前記第 1 の要素を第 3 の乱数および前記公開情報を用いて変換して第 2 の変換データを作成するステップと、

署名を付加すべきメッセージ、第 4 の乱数、前記暗号化データ、前記第 1 の変換データ、前記第 2 の変換データ、署名の作成に用いる秘密鍵である署名鍵、前記第 1 の要素、および前記第 2 の要素から、前記暗号化データ、前記第 1 の変換データ、および前記第 2 の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第 1 の要素、前記第 2 の要素、および前記署名鍵に関する情報を知られることのない知識署名データを作成するステップと、
25

前記暗号化データ、前記第 1 の変換データ、前記第 2 の変換データ、および前記知識署名データをグループ署名として前記メッセージと共に出力するステップ

と、

前記検証装置において、

メッセージおよびグループ署名と、前記グループ管理装置にて開示されている前記公開情報とから、前記グループ署名が、前記グループに登録されているい
5 らかのメンバーのメンバー証明書に含まれる第1の要素および第2の要素と前記署名鍵を用いて作成されたものか否かを、前記第1の要素、前記第2の要素、および前記署名鍵に関する情報を用いることなく検証するステップとを有するグループ署名方法。

10 11. システム内で共通に利用する公開情報を他の装置から参照可能に開示するグループ管理装置、およびグループ署名の署名者がグループのメンバーであるか否か確認する検証装置と共にグループ署名システムを構成し、前記署名者が前記グループに登録されたメンバーであることを証明することのできるグループ署名を作成するグループ署名装置であって、

15 第1の要素および第2の要素を含むメンバー証明書を記憶するメンバー情報記憶手段と、

前記第1の要素を第1の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成する暗号化データ作成手段と、

20 前記第1の要素を第2の乱数および前記公開情報を用いて変換して第1の変換データを作成する第1の変換データ作成手段と、

前記第1の要素を第3の乱数および前記公開情報を用いて変換して第2の変換データを作成する第2の変換データ作成手段と、

署名を付加すべきメッセージ、第4の乱数、前記暗号化データ、前記第1の変換データ、前記第2の変換データ、署名の作成に用いる秘密鍵である署名鍵、前
25 記第1の要素、および前記第2の要素から、前記暗号化データ、前記第1の変換データ、および前記第2の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第1の要素、前記第2の要素、および前記署名鍵に関する情報を知られることのない知識署名データを作成する知識署名作成手段と、

前記暗号化データ、前記第1の変換データ、前記第2の変換データ、および前

記知識署名データをグループ署名として前記メッセージと共に出力する署名出力手段とを有するグループ署名装置。

1 2. システム内で共通に利用する公開情報を他の装置から参照可能に開示するグループ管理装置、およびグループ署名の署名者がグループのメンバーである
5 否か確認する検証装置と共にグループ署名システムを構成するグループ署名装置として動作させ、前記署名者が前記グループに登録されたメンバーであることを証明することのできるグループ署名を作成させるために、コンピュータに実行させるグループ署名プログラムであって、

10 メンバー情報記憶手段が、第1の要素および第2の要素を含むメンバー証明書を記憶する処理と、

暗号化データ作成手段が、前記第1の要素を第1の乱数と前記グループ管理装置にて開示されている前記公開情報とを用いて暗号化して暗号化データを作成する処理と、

15 第1の変換データ作成手段が、前記第1の要素を第2の乱数および前記公開情報を用いて変換して第1の変換データを作成する処理と、

第2の変換データ作成手段が、前記第1の要素を第3の乱数および前記公開情報を用いて変換して第2の変換データを作成する処理と、

知識署名作成手段が、署名を付加すべきメッセージ、第4の乱数、前記暗号化データ、前記第1の変換データ、前記第2の変換データ、署名の作成に用いる秘密鍵である署名鍵、前記第1の要素、および前記第2の要素から、前記暗号化データ、前記第1の変換データ、および前記第2の変換データが同じ値を元に作成されていることを証明可能でありかつ前記第1の要素、前記第2の要素、および前記署名鍵に関する情報を知られることのない知識署名データを作成する処理と、

20 署名出力手段が、前記暗号化データ、前記第1の変換データ、前記第2の変換データ、および前記知識署名データをグループ署名として前記メッセージと共に出力する処理とを有するグループ署名プログラム。

図 1

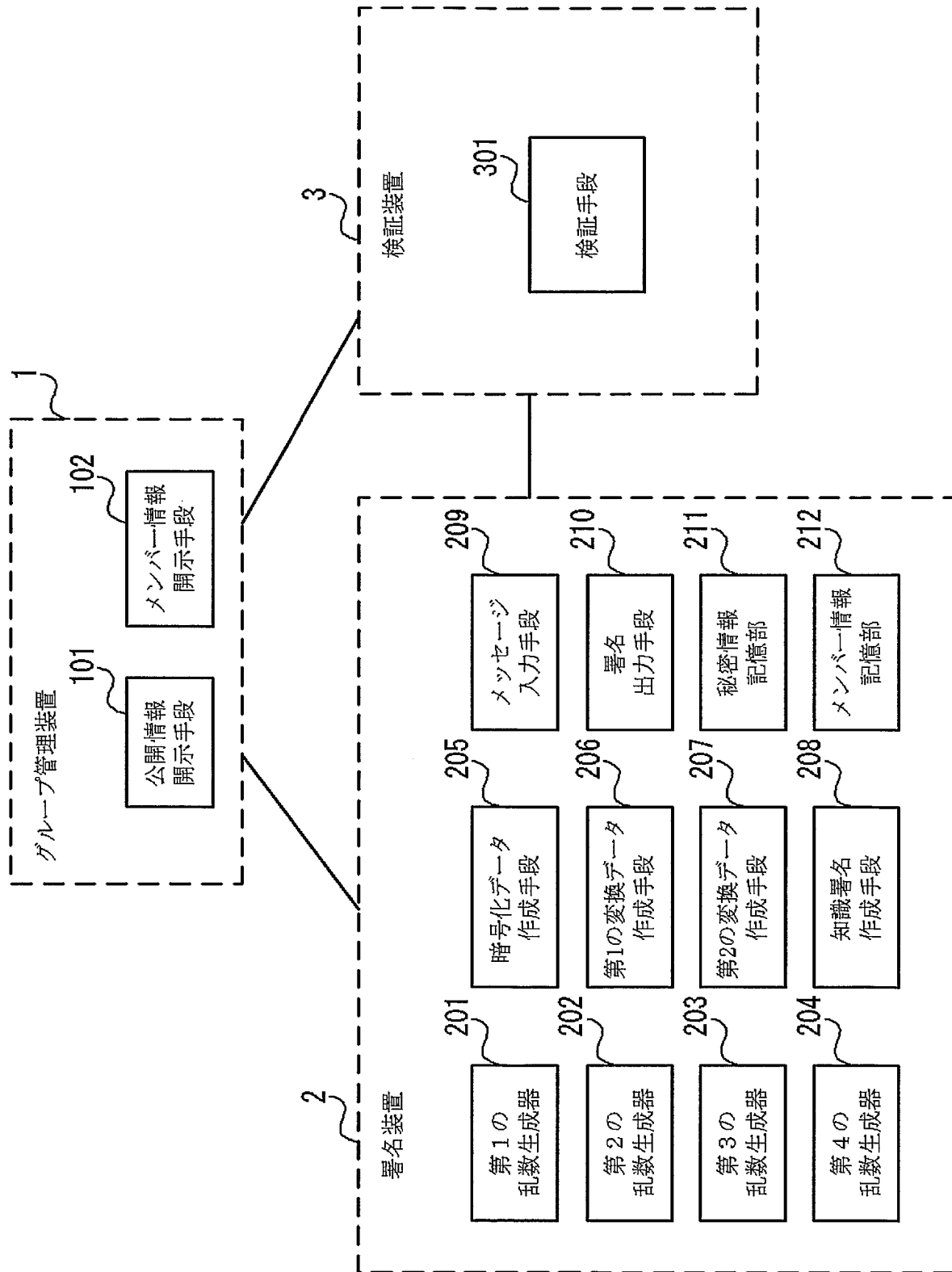
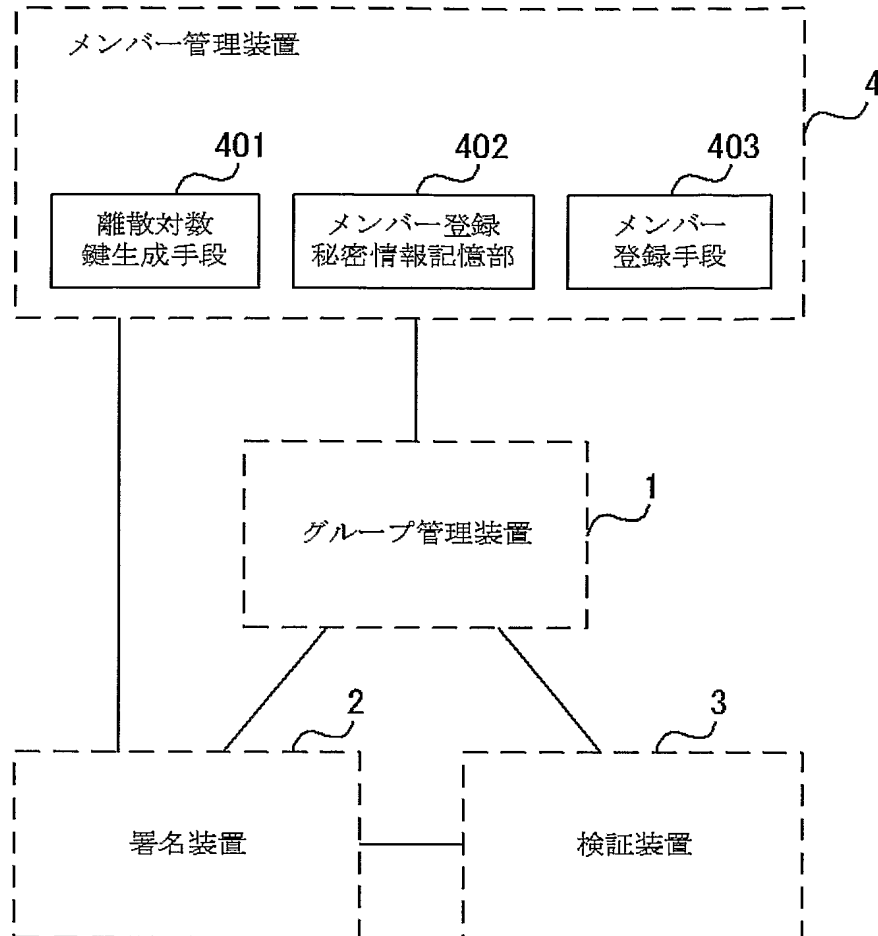


図 2



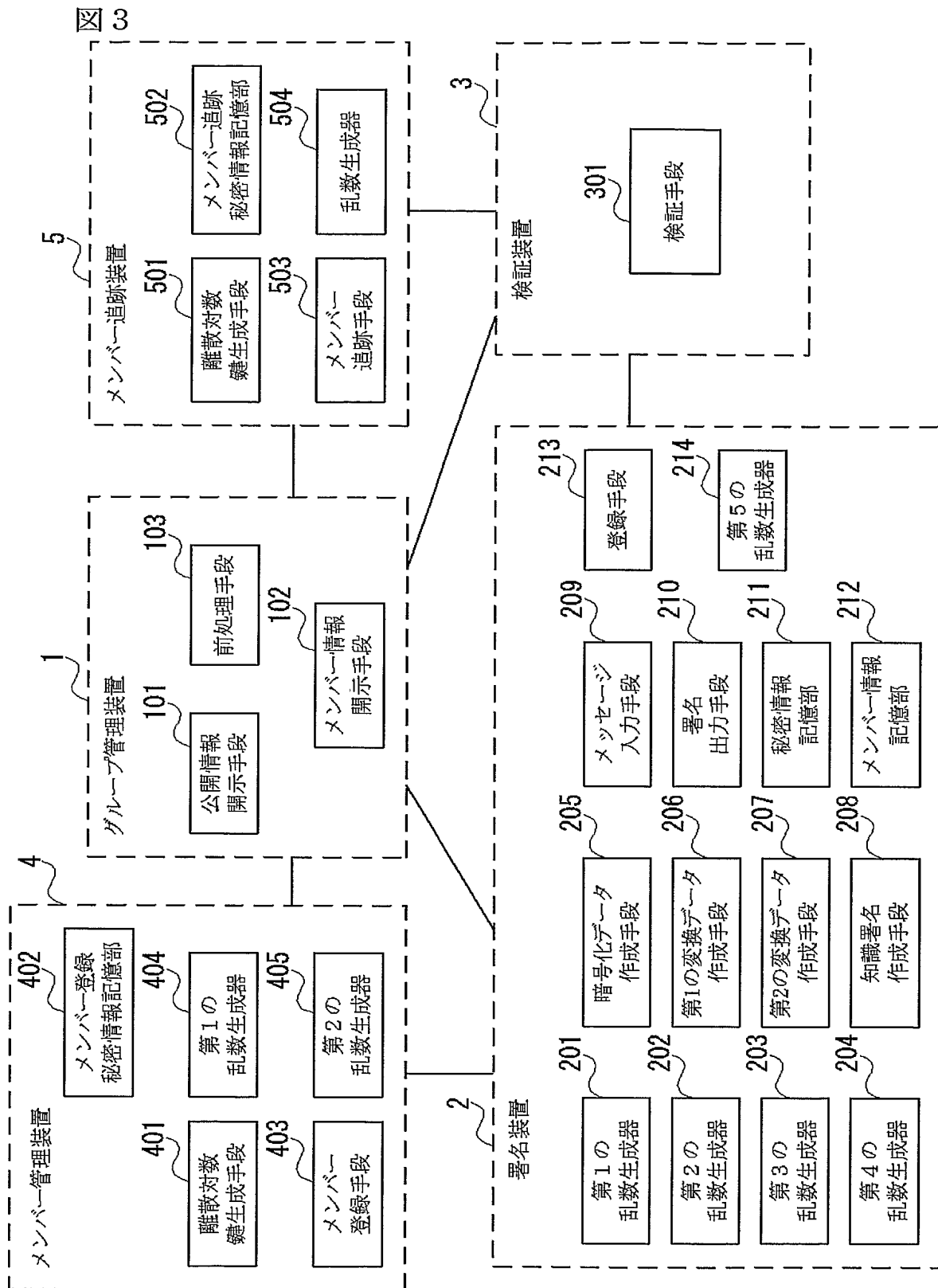


図 4

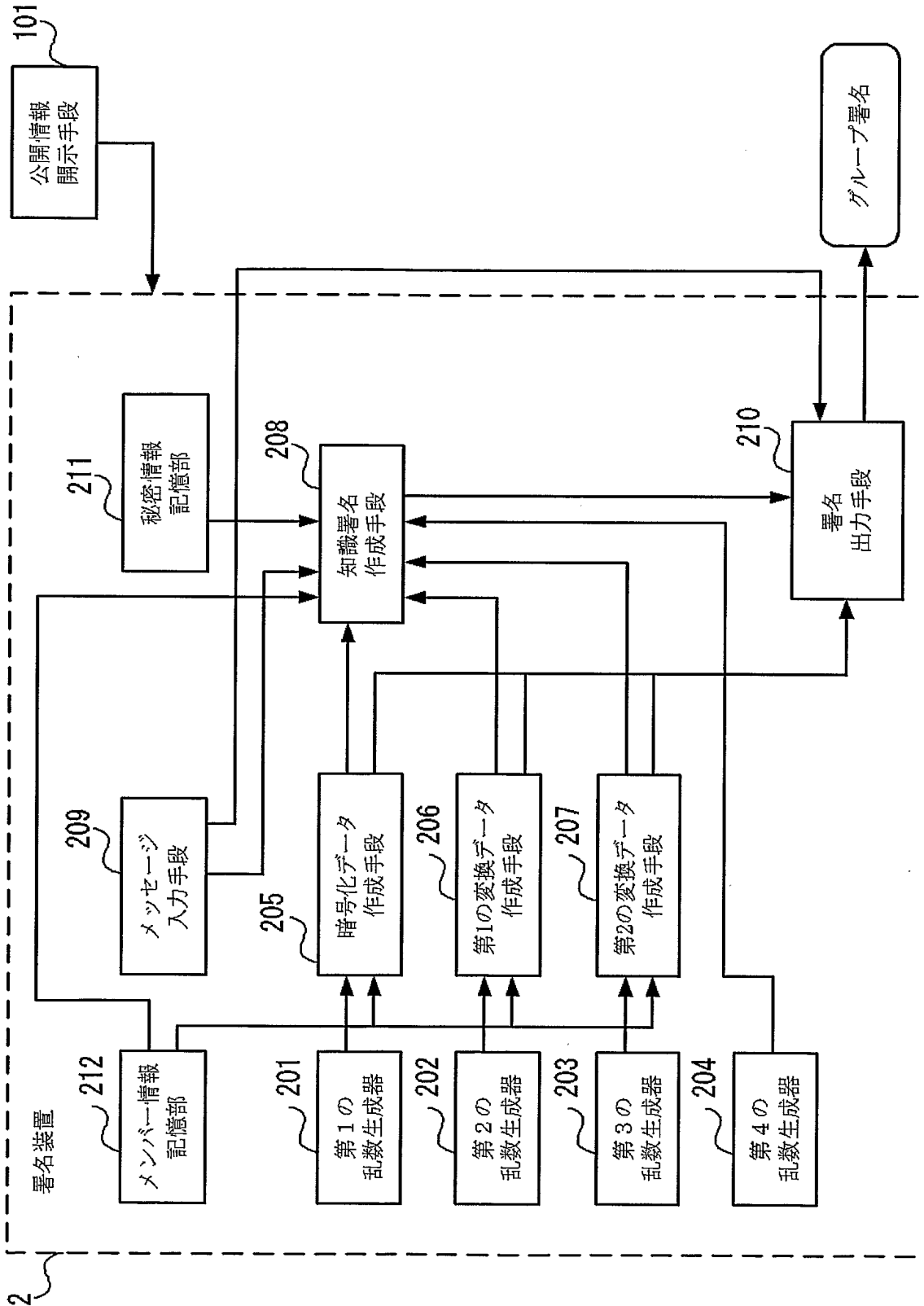


図 5

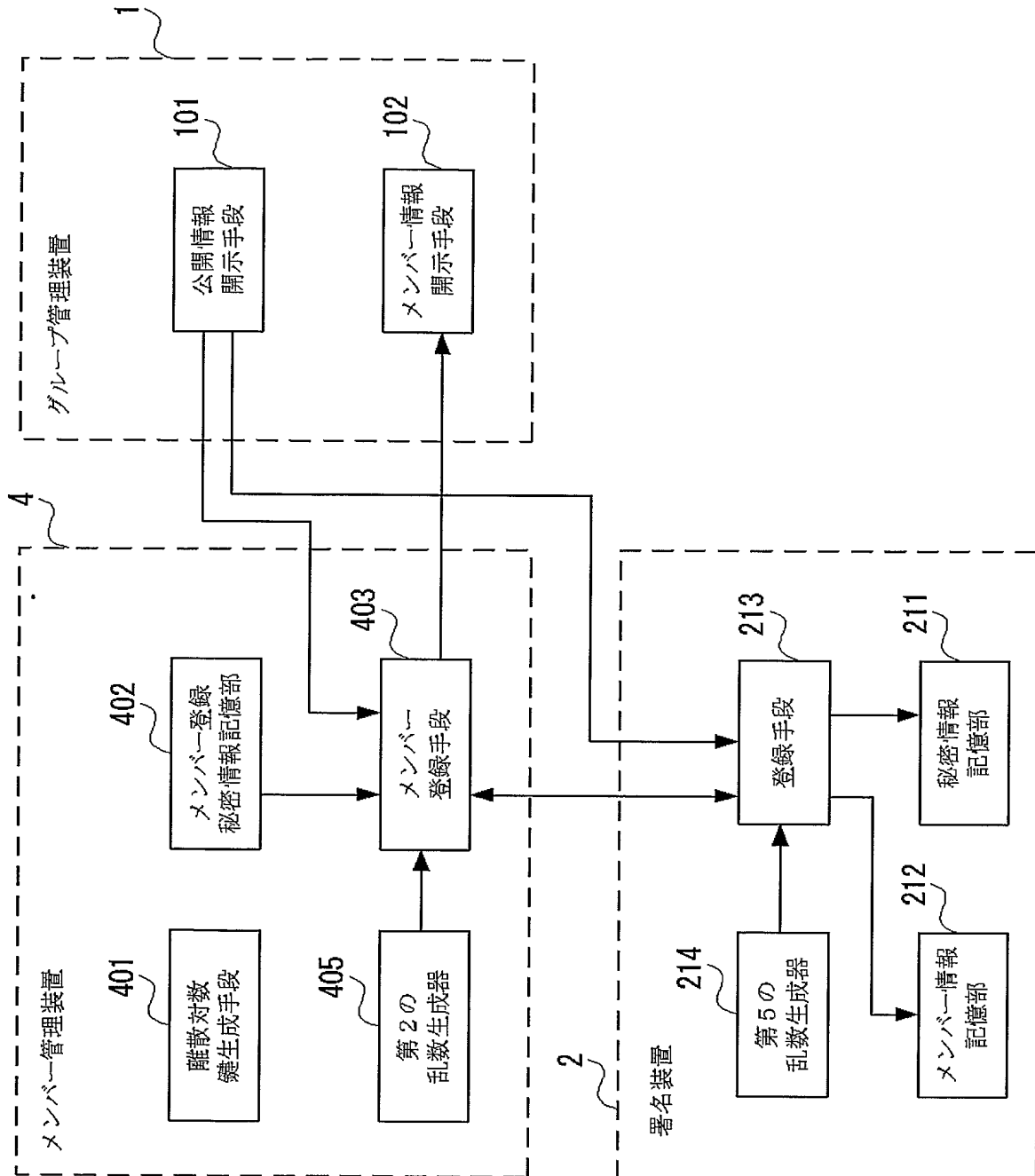


図 6

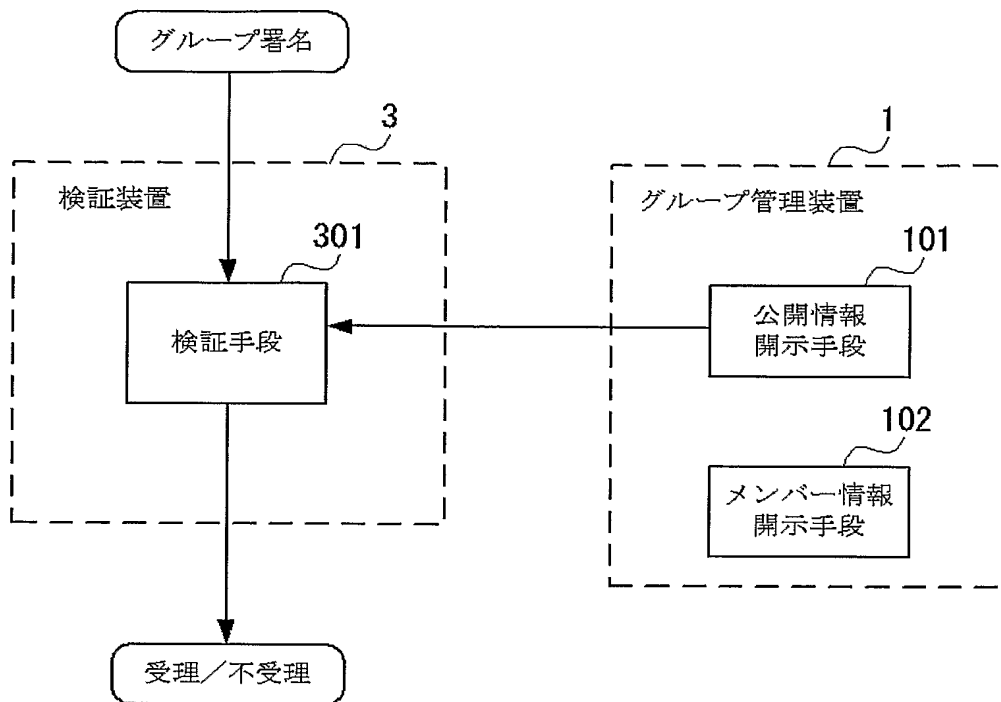


図 7

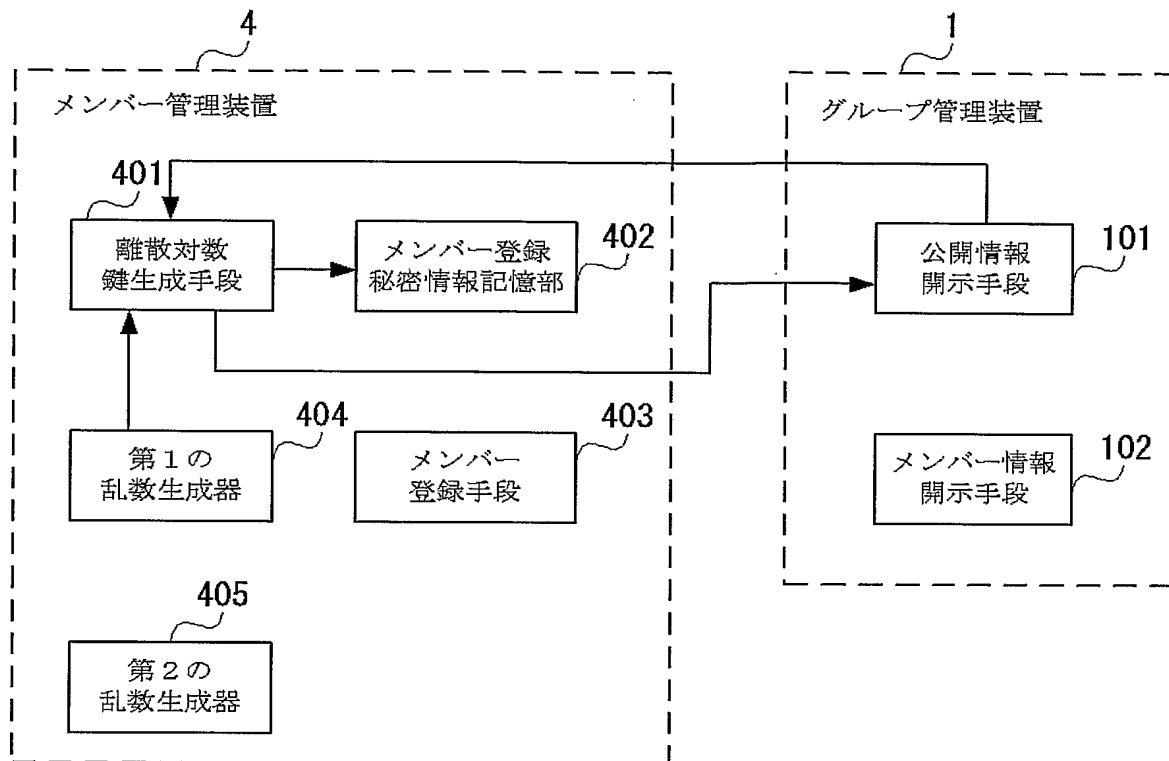


図 8

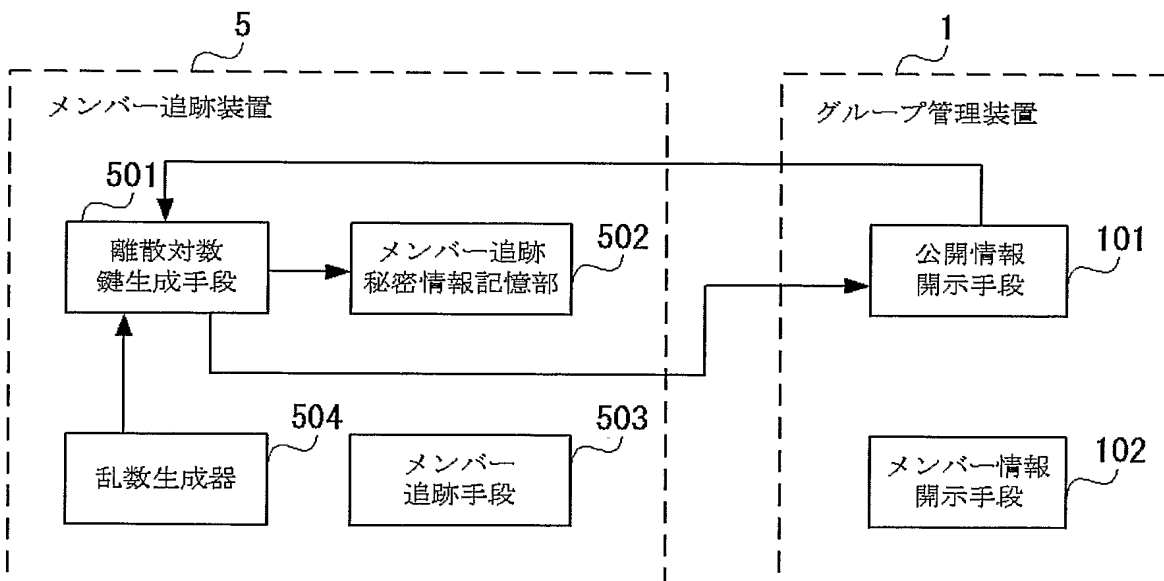


図 9

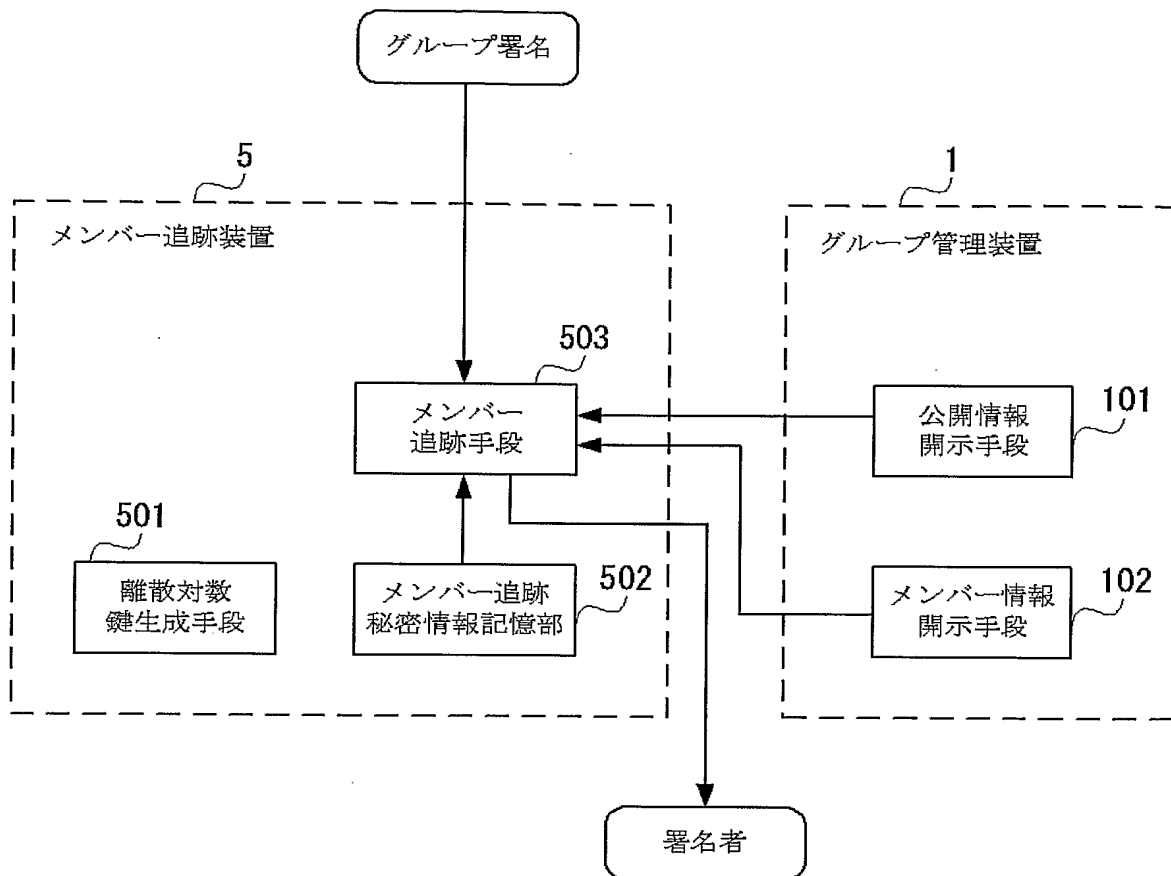


図 10

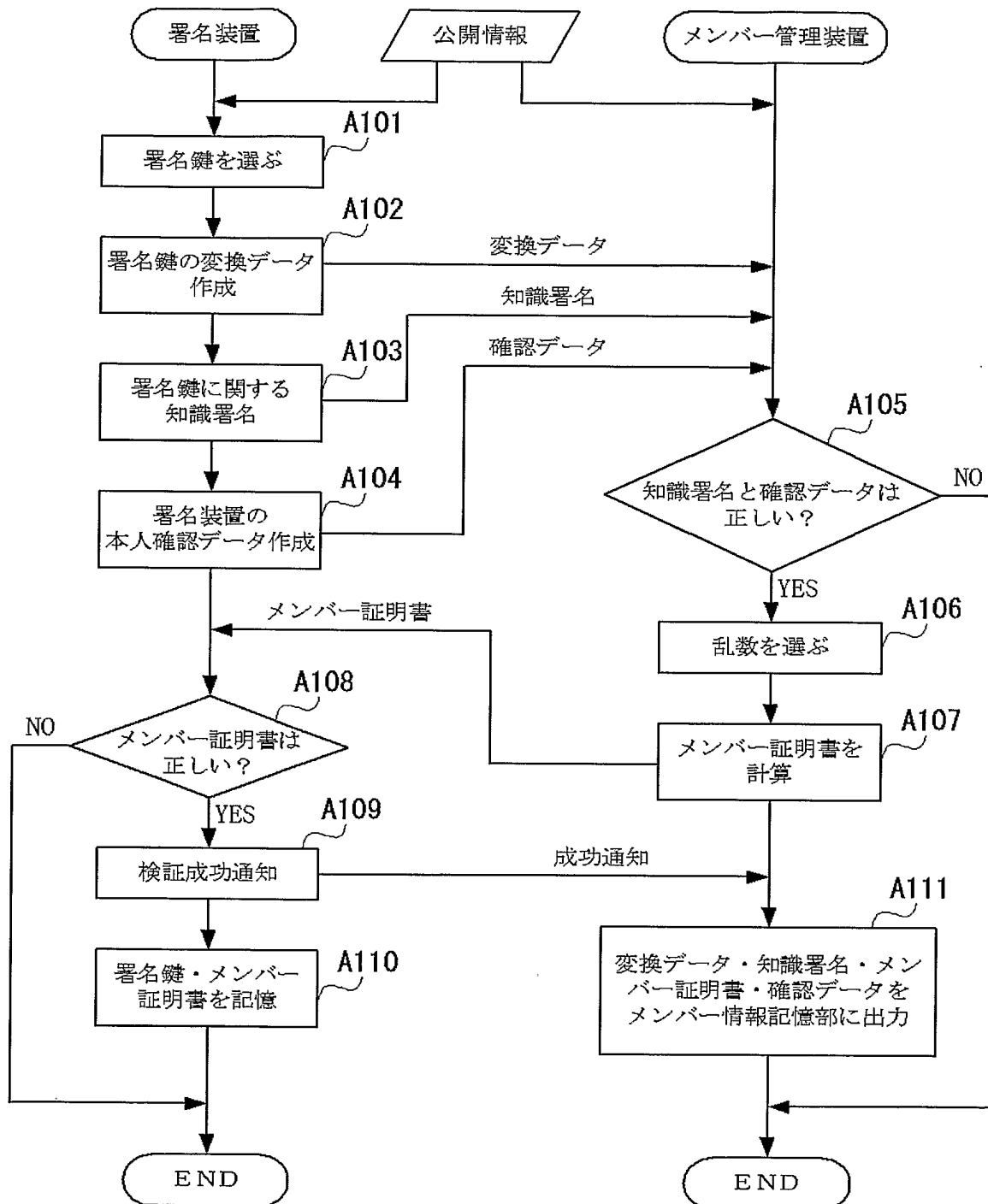


図 1 1

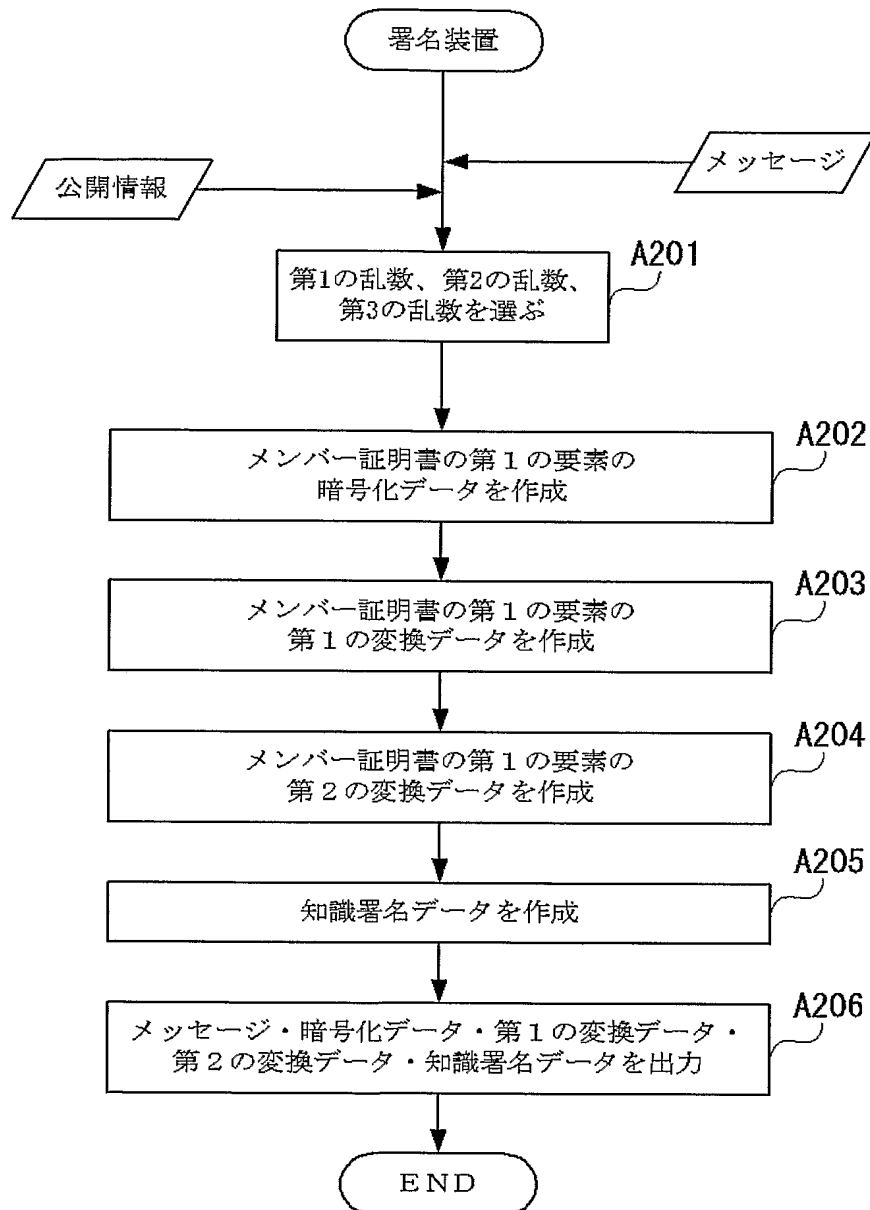


図 12

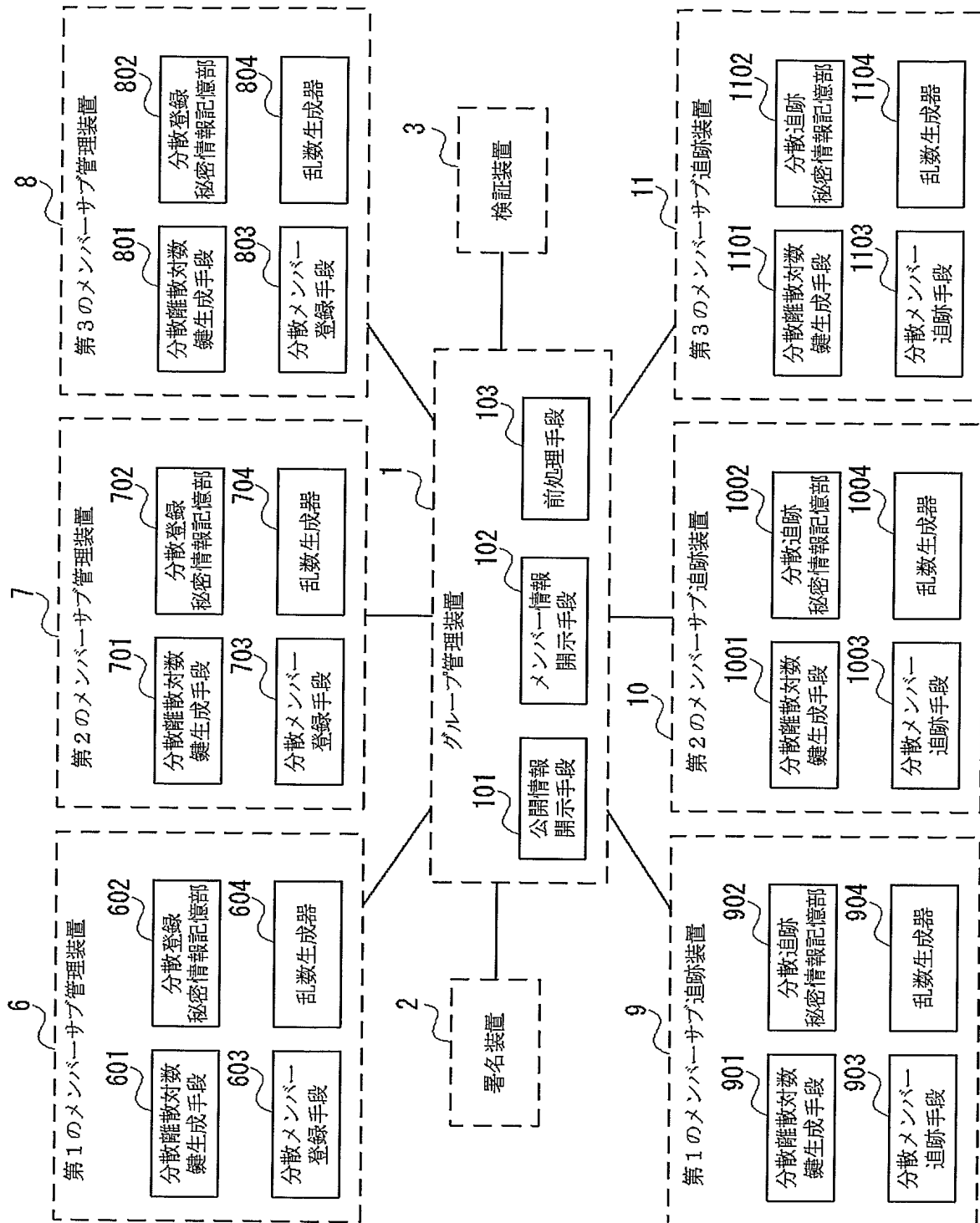
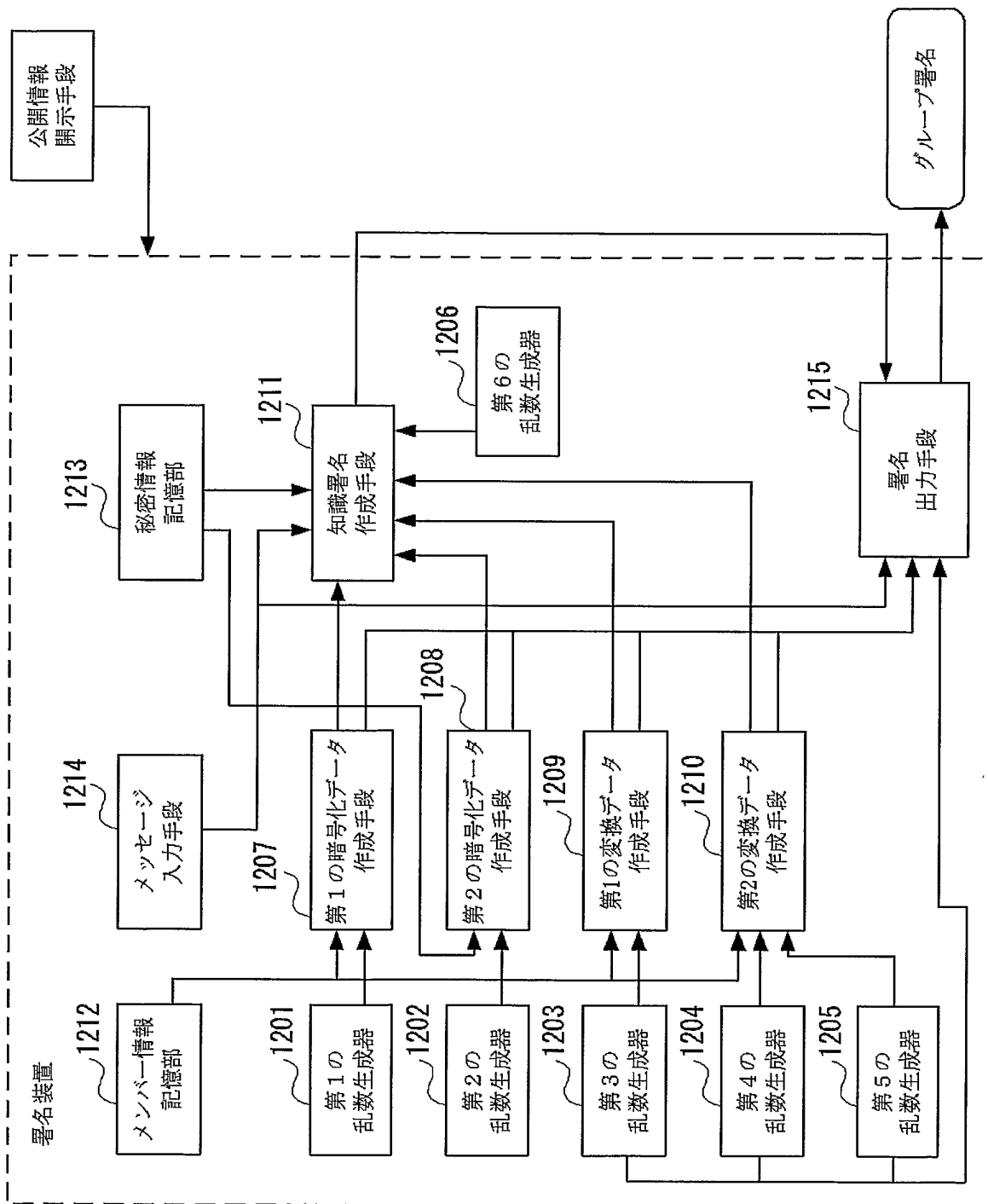


図 13



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/001177

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl.⁷ H04L9/32, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.⁷ H04L9/32, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Jitsuyo Shinan Toroku Koho	1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS), WPI, INSPEC (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Kozue Umeda, Atsuko Miyaji, "A Group Signature Scheme based on Nyberg-Ryeppele Signatures", 2003 Nen Anko to Joho Security Symposium Yokoshu, Vol.1 of 2, 26 January, 2003 (26.01.03), pages 327 to 332	1-12
Y	Takamitsu KATO, Shoichi HIROSE, Michihiko MINO, Katsuo IKEDA, "ElGamal no Kokai Kagi Angokei ni Motozuku Group Shomei ni yoru Shomei Protocol", 1992 Nen The Institute of Electronics, Information and Communication Engineers - Soritsu 75 Shunen Kinen - Shuki Taikai Koen Ronbunshu, separate Vol.1, 15 September, 1992 (15.09.92), page 1-187	1-12

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
26 April, 2005 (26.04.05)

Date of mailing of the international search report
17 May, 2005 (17.05.05)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/001177

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	Shoko YONEZAWA, Jun FURUKAWA, "Kanrisha Bunsan ni Tekishita Group Shomei Hoshiki", 2004 Nen Ango to Joho Security Symposium Yokoshu, Vol.2 of 2, 27 January, 2004 (27.01.04), pages 1167 to 1172	1-12

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/32, G09C1/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/32, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国登録実用新案公報	1994-2005年
日本国実用新案登録公報	1996-2005年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS), WPI, INSPEC (DIALOG)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	Kozue Umeda, Atsuko Miyaji, "A Group Signature Scheme based on Nyberg-Ryeppele Signatures", 2003年暗号と情報セキュリティシンポジウム予稿集, Volume 1 of 2, 2003. 01. 26, p. 327-332	1-12
Y	加藤隆充, 廣瀬勝一, 美濃導彦, 池田克夫, "El Gamalの公開鍵暗号系に基づくグループ署名による署名プロトコル", 1992年電子情報通信学会一創立75周年記念一秋季大会講演論文集, 分冊1, 1992. 09. 15, p. 1-187	1-12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

26. 04. 2005

国際調査報告の発送日

17. 5. 2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
P, X	米沢祥子, 古川潤, “管理者分散に適したグループ署名方式”, 2004年暗号と情報セキュリティシンポジウム予稿集, Volume 2 of 2, 2004. 01. 27, p. 1167-1172	1-12